ORACLE
Linux

FIPS 140-3 Non-Proprietary Security Policy

Oracle Corporation

Oracle Linux 8 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module and Oracle Linux 9 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module

Software Versions: kernel: 5.15.0-303.171.5.2.2.el8uek and 5.15.0-303.171.5.2.2.el9uek

libkcapi: 1.2.0-2.0.1.el8 and 1.3.1-3.0.1.el9

Date: September 1, 2026

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

©Oracle Corporation
This document may be reproduced whole and intact including the Copyright notice.

Title: Oracle Linux 8 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module and Oracle Linux 9 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module Security Policy

Date: September 1st, 2026

Contributing Authors:

Oracle Linux Engineering

Security Evaluations – Global Product Security

atsec information security

Oracle Corporation

World Headquarters

2300 Oracle Way

Austin, TX 78741

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

www.oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Oracle specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may be reproduced or distributed whole and intact including this copyright notice.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Hardware and Software, Engineered to Work Together

ORACLE

Table of Contents

1 General 1

1.1 Overview 1

1.1.1. How This Security Policy was Prepared 1

1.2 Security Levels 1

1.3 Additional Information 1

2 Cryptographic Module Specification 3

2.1 Description 3

2.2 Tested and Vendor Affirmed Module Version and Identification 4

2.3 Excluded Components 5

2.4 Modes of Operation 5

2.5 Algorithms 5

2.6 Security Function Implementations 11

2.7 Algorithm Specific Information 16

2.7.1 AES GCM IV 16

2.7.2 RSA 16

2.7.3 AES XTS 16

2.7.4 SP 800-56Ar3 Assurances 17

2.7.5 SHA3 17

2.7.6 Key Agreement and Key Transport 17

2.7.7 SHA-1 17

2.8 RBG and Entropy 17

2.9 Key Generation 18

2.10 Key Establishment 18

2.11 Industry Protocols 18

3 Cryptographic Module Interfaces 19

3.1 Ports and Interfaces 19

4 Roles, Services, and Authentication 20

4.1 Authentication Methods 20

4.2 Roles 20

4.3 Approved Services 20

4.4 Non-Approved Services 24

4.5 External Software/Firmware Loaded 24

5 Software/Firmware Security 25

5.1 Integrity Techniques 25

5.2 Initiate on Demand 25

6 Operational Environment 26

6.1 Operational Environment Type and Requirements 26
6.2 Configuration Settings and Restrictions 26
7 Physical Security 27
8 Non-Invasive Security 28
9 Sensitive Security Parameters Management 29
9.1 Storage Areas 29
9.2 SSP Input-Output Methods 29
9.3 SSP Zeroization Methods 29
9.4 SSPs 29
9.5 Transitions 34
10 Self-Tests 35
10.1 Pre-Operational Self-Tests 35
10.2 Conditional Self-Tests 35
10.3 Periodic Self-Test Information 76
10.4 Error States 87
10.5 Operator Initiation of Self-Tests 87
11 Life-Cycle Assurance 88
11.1 Startup Procedures 88
11.2 Administrator Guidance 89
11.3 Non-Administrator Guidance 89
11.4 Maintenance Requirements 89
11.5 End of Life 89
12 Mitigation of Other Attacks 90
Appendix A Glossary and Abbreviations 91
Appendix B References 92

ORACLE

List of Tables

Table 1: Security Levels....1
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)....4
Table 3: Tested Operational Environments - Software, Firmware, Hybrid....4
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid....5
Table 5: Modes List and Description....5
Table 6: Approved Algorithms....10
Table 7: Vendor-Affirmed Algorithms....11
Table 8: Non-Approved, Not Allowed Algorithms....11
Table 9: Security Function Implementations....16
Table 10: Entropy Certificates....17
Table 11: Entropy Sources....17
Table 12: Ports and Interfaces....19
Table 13: Roles....20
Table 14: Approved Services....23
Table 15: Non-Approved Services....24
Table 16: Storage Areas....29
Table 17: SSP Input-Output Methods....29
Table 18: SSP Zeroization Methods....29
Table 19: SSP Table 1....31
Table 20: SSP Table 2....33
Table 21: Pre-Operational Self-Tests....35
Table 22: Conditional Self-Tests....76
Table 23: Pre-Operational Periodic Information....76
Table 24: Conditional Periodic Information....87
Table 25: Error States....87

List of Figures

Figure 1: Block Diagram....3

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for Oracle Linux 8 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module and Oracle Linux 9 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module versions:

- kernel: 5.15.0-303.171.5.2.2.el8uek and 5.15.0-303.171.5.2.2.el9uek;
- libkcapi: 1.2.0-2.0.1.el8 and 1.3.1-3.0.1.el9

It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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

1.1.1. How This Security Policy was Prepared

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

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

This Security Policy describes the features and design of the module named GnuTLS Cryptographic Module using the terminology contained in the FIPS 140-3 specification. The FIPS 140-3 Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic module to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

This document may be reproduced and distributed only whole and intact, including the Copyright notice

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 Oracle Linux 8 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module and Oracle Linux 9 Unbreakable Enterprise Kernel (UEK7) Cryptographic Module (hereafter referred to as "the module") provides a C language application program interface (API) for use by other (kernel space and user space) processes that require cryptographic functionality. The module operates on a general-purpose computer as part of the Linux kernel. Its cryptographic functionality can be accessed using the Linux Kernel Crypto API.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

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

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is defined as the general-purpose computer on which the module is installed.

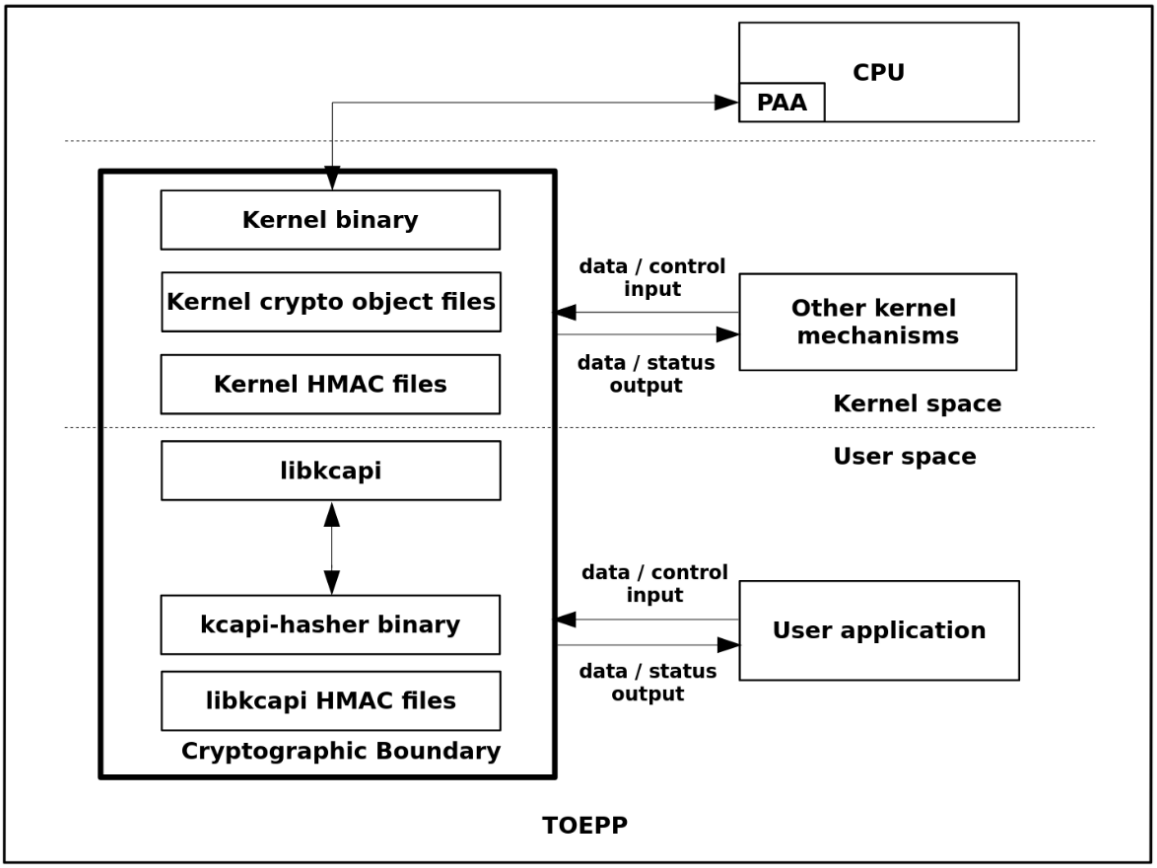


Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
kernel and libkcapi.so on Oracle Linux 8 on KVM on Oracle Linux 8 on ORACLE SERVER X9-2c with Intel(R) Xeon(R) Platinum 8358	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 9 on KVM on Oracle Linux 8 on ORACLE SERVER X9-2c with Intel(R) Xeon(R) Platinum 8358	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 8 on KVM on Oracle Linux 8 on ORACLE SERVER E4-2c with AMD EPYC 7J13	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 9 on KVM on Oracle Linux 8 on ORACLE SERVER E4-2c with AMD EPYC 7J13	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 8 on KVM on Oracle Linux 8 on ORACLE SERVER A1-2c with Ampere(R) Altra(R) Q80-30	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 9 on KVM on Oracle Linux 8 on ORACLE SERVER A1-2c with Ampere(R) Altra(R) Q80-30	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9	N/A	HMAC-SHA-512
kernel and libkcapi.so on Oracle Linux 9 on KVM on Oracle Linux 8 on Marvell Liquid IO II (MIPS64) SmartNIC with OCTEON III	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9	N/A	HMAC-SHA-512

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

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Oracle Linux 8	ORACLE SERVER X9-2c	Intel® Xeon® Platinum 8358	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 8	ORACLE SERVER E4-2c	AMD EPYC 7J13	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 8	ORACLE SERVER A1-2c	Ampere® Altra® Q80-30	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 9	ORACLE SERVER X9-2c	Intel® Xeon® Platinum 8358	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 9	ORACLE SERVER E4-2c	AMD EPYC 7J13	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 9	ORACLE SERVER A1-2c	Ampere® Altra® Q80-30	Yes	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 8	ORACLE SERVER X9-2c	Intel® Xeon® Platinum 8358	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 8	ORACLE SERVER E4-2c	AMD EPYC 7J13	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 8	ORACLE SERVER A1-2c	Ampere® Altra® Q80-30	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el8uek; 1.2.0-2.0.1.el8
Oracle Linux 9	ORACLE SERVER X9-2c	Intel® Xeon® Platinum 8358	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 9	ORACLE SERVER E4-2c	AMD EPYC 7J13	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 9	ORACLE SERVER A1-2c	Ampere® Altra® Q80-30	No	KVM on Oracle Linux 8	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9
Oracle Linux 9	Marvell Liquid IO II (MIPS64) SmartNIC	Marvell OCTEON III	No	N/A	5.15.0-303.171.5.2.2.el9uek; 1.3.1-3.0.1.el9

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

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

Operating System	Hardware Platform
Oracle Linux 8	Oracle X Series Servers
Oracle Linux 8	Oracle E Series Servers
Oracle Linux 8	Oracle A Series Servers
Oracle Linux 8	Marvell T93 LiquidIO III (ARM v8.x) SmartNIC
Oracle Linux 8	Pensando DSC-200-R (ARM v8.x) SmartNIC
Oracle Linux 8	Nvidia Bluefield-3 (ARM v8.x) SmartNIC
Oracle Linux 9	Oracle X Series Servers
Oracle Linux 9	Oracle E Series Servers
Oracle Linux 9	Oracle A Series Servers
Oracle Linux 9	Marvell T93 LiquidIO III (ARM v8.x) SmartNIC
Oracle Linux 9	Pensando DSC-200-R (ARM v8.x) SmartNIC
Oracle Linux 9	Nvidia Bluefield-3 (ARM v8.x) SmartNIC

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

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

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service as defined in section 4.3
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service as defined in section 4.4

Table 5: Modes List and Description

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode.

Mode change instructions and status indicators:

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:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CBC-CS3	A3866, A3874, A3884, A3889, A3891, A4166, A4174, A4176, A4178, A4188	Direction - decrypt, encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128-65536 Increment 8	SP 800-38A
AES-CCM	A3862, A3869, A3879, A3889, A3891, A4176, A4178, A4183	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CCM	A4162, A4169	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-524288 Increment 8, AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB128	A3864, A3872, A3882, A3891, A4164, A4172, A4178, A4186	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3862, A3869, A3879, A3889, A3891, A4162, A4169, A4176, A4178, A4183	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B
AES-CTR	A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3889, A3891, A3892, A3893, A3894, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4176, A4178, A4179, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3862, A3869, A3879, A3891, A4178, A4183	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		IV Length - IV Length: 96 Payload Length - Payload Length: 128-65536 Increment 128 AAD Length - AAD Length: 128, 256, 120, 0	
AES-GCM	A3867, A3870, A3877, A3880, A3892, A4167, A4170, A4181, A4184, A4196	Direction - Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-GCM	A3868, A3871, A3876, A3878, A3881, A3893, A4168, A4171, A4182, A4185, A4191, A4197	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 64, 96	SP 800-38D
AES-GCM	A4162, A4169	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128-65536 Increment 128 AAD Length - AAD Length: 0-65536 Increment 8, AAD Length: 128, 256, 120, 0	SP 800-38D
AES-GMAC	A3862, A3869, A3879, A3891, A4178, A4183	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 AAD Length - AAD Length: 128, 256, 120, 0	SP 800-38D
AES-GMAC	A4162, A4169	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		AAD Length - AAD Length: 0-65536 Increment 8, AAD Length: 128, 256, 120, 0	
AES-OFB	A3865, A3873, A3883, A3891, A4165, A4173, A4178, A4187	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4176, A4178, A4179, A4183, A4191	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A4162, A4169	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128, Payload Length: 128-65536 Increment 8 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3891, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4178, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 128, Entropy Input: 192, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64 Personalization String Length - Personalization String Length: 0 Returned Bits - 1024, 4096, 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3861, A4161	Curve - P-256, P-384 Secret Generation Mode - Testing Candidates	FIPS 186-4
Hash DRBG	A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3885, A3886, A3887, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4181, A4182, A4183, A4184, A4185, A4189, A4190, A4191, A4192, A4196, A4197	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-512 Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0,	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		256 Returned Bits - 1024, 2048, 320	
HMAC DRBG	A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3885, A3886, A3887, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4181, A4182, A4183, A4184, A4185, A4189, A4190, A4191, A4192, A4196, A4197	Prediction Resistance - No, Yes Supports Reseed - No Mode - SHA-1, SHA2-256, SHA2-512 Entropy Input - Entropy Input: 160, Entropy Input: 256 Nonce - Nonce: 160, Nonce: 256 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 320	SP 800-90A Rev. 1
HMAC-SHA-1	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189, A4190, A4192, A4193, A6709	MAC - MAC: 160 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A3863, A4163	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A3863, A4163	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A3863, A4163	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A3863, A4163	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3861, A4161	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3860, A4160	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme -	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		dhEphem - KAS Role - initiator, responder	
RSA SigVer (FIPS186-4)	A3862, A3885, A3886, A3887, A4162, A4189, A4190, A4192	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
Safe Primes Key Generation	A3860, A4160	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA-1	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189, A4190, A4192, A4193	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA-1	A6709	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-224	A6709	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-256	A6709	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-384	A6709	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 180-4
SHA2-512	A6709	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A3863, A4163	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-256	A3863, A4163	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-384	A3863, A4163	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202
SHA3-512	A3863, A4163	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Cryptographic Key Generation (CKG)		N/A	SP 800-133Rev2 section 4, example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

The module does not implement non-approved algorithms allowed in the approved mode of operation.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

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

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Shared Secret Computation	KAS-SSC	SP 800-56Ar3. KAS-ECC-SSC and KAS-FFC-SSC per IG D.F Scenario 2, path (1)	KAS-ECC-SSC Sp800-56Ar3 strength:128-192 bits KAS-FFC-SSC Sp800-56Ar3 strength:112-200 bits	KAS-ECC-SSC Sp800-56Ar3: (A3861, A4161) KAS-FFC-SSC Sp800-56Ar3: (A3860, A4160)
Authenticated Encryption with AES-CBC or AES-CTR with HMAC	BC-Auth	SP800-38A, FIPS 198-1. Authenticated encryption		AES-CBC: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-CTR: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) HMAC-SHA-1: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189, A4190, A4192, A4193, A6709) HMAC-SHA2-256: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-384: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) HMAC-SHA2-512: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709)
Authenticated Decryption with AES-CBC or AES-CTR with HMAC	BC-Auth	SP800-38A, FIPS 198-1. Authenticated decryption		AES-CBC: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-CTR: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) HMAC-SHA-1: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189, A4190, A4192, A4193, A6709) HMAC-SHA2-256: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709) HMAC-SHA2-384: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) HMAC-SHA2-512: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709)
Hashing	SHA	FIPS180-4, FIPS202. Message digest		SHA-1: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189, A4190, A4192, A4193, A6709) SHA2-224: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709) SHA2-256: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) SHA2-512: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) SHA3-224: (A3863, A4163) SHA3-256: (A3863, A4163) SHA3-384: (A3863, A4163) SHA3-512: (A3863, A4163)
Encryption	BC-UnAuth	SP800-38A. Encryption		AES-CBC: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-CBC-CS3: (A3866, A3874, A3884, A3889, A3891, A4166, A4174, A4176, A4178, A4188) AES-CFB128: (A3864, A3872, A3882, A3891, A4164, A4172, A4178, A4186) AES-CTR: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-ECB: (A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3889, A3891, A3892, A3893, A3894, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4176, A4178, A4179, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197) AES-OFB: (A3865, A3873, A3883, A3891, A4165, A4173, A4178, A4187) AES-XTS Testing Revision 2.0: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191)
Decryption	BC-UnAuth	SP800-38A. Decryption		AES-CBC: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-CBC-CS3: (A3866, A3874, A3884, A3889, A3891, A4166, A4174, A4176, A4178, A4188) AES-CFB128: (A3864, A3872, A3882,

Name	Type	Description	Properties	Algorithms
				A3891, A4164, A4172, A4178, A4186) AES-CTR: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191) AES-ECB: (A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3889, A3891, A3892, A3893, A3894, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4176, A4178, A4179, A4181, A4182, A4183, A4184, A4185, A4191, A4196) AES-OFB: (A3865, A3873, A3883, A3891, A4165, A4173, A4178, A4187) AES-XTS Testing Revision 2.0: (A3862, A3869, A3876, A3879, A3889, A3891, A3894, A4162, A4169, A4176, A4178, A4179, A4183, A4191)
Authenticated Encryption	BC-AuthEncrypt	SP800-38C, SP800-38D. Authenticated encryption		AES-CCM: (A3862, A3869, A3879, A3889, A3891, A4162, A4169, A4176, A4178, A4183) AES-GCM: (A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3891, A3892, A3893, A4162, A4167, A4168, A4169, A4170, A4171, A4178, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197)
Authenticated Decryption	BC-AuthDecrypt	SP800-38C, SP800-38D. Authenticated decryption		AES-CCM: (A3862, A3869, A3879, A3889, A3891, A4162, A4169, A4176, A4178, A4183) AES-GCM: (A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3891, A3892, A3893, A4162, A4167, A4168, A4169, A4170, A4171, A4178, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197)
Message Authentication	MAC	SP800-38B, SP800-38D, FIPS 198-1. Message authentication		AES-CMAC: (A3862, A3869, A3879, A3889, A3891, A4162, A4169, A4176, A4178, A4183) AES-GMAC: (A3862, A3869, A3879, A3891, A4162, A4169, A4178, A4183) HMAC-SHA-1: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A4160, A4161, A4162, A4176, A4189,

Name	Type	Description	Properties	Algorithms
				A4190, A4192, A4193, A6709) HMAC-SHA2-224: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709) HMAC-SHA2-256: (A3860, A3861, A3862, A3885, A3886, A3887, A3888, A3889, A3894, A3895, A4160, A4161, A4162, A4176, A4179, A4180, A4189, A4190, A4192, A4193, A6709) HMAC-SHA2-384: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) HMAC-SHA2-512: (A3860, A3861, A3862, A3885, A3886, A3887, A3890, A3895, A4160, A4161, A4162, A4177, A4180, A4189, A4190, A4192, A6709) HMAC-SHA3-224: (A3863, A4163) HMAC-SHA3-256: (A3863, A4163) HMAC-SHA3-384: (A3863, A4163) HMAC-SHA3-512: (A3863, A4163)
Key Generation	AsymKeyPair-KeyGen CKG	FIPS186-4, SP800-56Ar3. ECDSA Key pair generation according to FIPS186-4, Appendix B.4.2 per IG D.H; Safe Primes Key Generation according to SP800-56Ar3, Section 5.6.1.1.4 per IG D.H		ECDSA KeyGen (FIPS186-4): (A3861, A4161) Safe Primes Key Generation: (A3860, A4160) Cryptographic Key Generation (CKG): ()
Random Numbers	DRBG	SP800-90Ar1. Random number generation		Counter DRBG: (A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3891, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4178, A4181, A4182, A4183, A4184, A4185, A4191, A4196, A4197) Hash DRBG: (A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871, A3876, A3877, A3878, A3879, A3880, A3881, A3885, A3886, A3887, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4181, A4182, A4183, A4184, A4185, A4189, A4190, A4191, A4192, A4196, A4197) HMAC DRBG: (A3860, A3861, A3862, A3867, A3868, A3869, A3870, A3871,

Name	Type	Description	Properties	Algorithms
				A3876, A3877, A3878, A3879, A3880, A3881, A3885, A3886, A3887, A3892, A3893, A4160, A4161, A4162, A4167, A4168, A4169, A4170, A4171, A4181, A4182, A4183, A4184, A4185, A4189, A4190, A4191, A4192, A4196, A4197)
RSA Signature Verification (Legacy)	DigSig-SigVer	FIPS 186-4. RSA Signature Verification.		RSA SigVer (FIPS186-4): (A4162, A4189, A4190, A4192, A3862, A3885, A3886, A3887)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

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

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

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

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

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

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

2.7.2 RSA

For RSA signature verification, the module supports modulus sizes 2048, 3072, and 4096 bits compliant to IG C.F. All supported modulus sizes have been CAVP tested. CAVP testing performed on the module's legacy implementations, specifically digital signature verification using SHA-1, were not testable under FIPS 186-5, but have been tested under FIPS 186-4 per IG C.K additional comment 2.

2.7.3 AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E. To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical.

Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3.

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

2.7.4 SP 800-56Ar3 Assurances

To comply with the assurances found in Section 5.6.2 of SP 800-56Ar3, the operator must use elliptic curve Diffie-Hellman shared secret computation algorithm with Bluetooth protocol. Additionally, the module's approved key pair generation service must be used to generate ephemeral Diffie-Hellman or EC Diffie-Hellman key pairs, or the key pairs must be obtained from another FIPS-validated module. As part of this service, the module will internally perform the full public key validation of the generated public key.

The module's shared secret computation service will internally perform the full public key validation of the peer DH public key, and the partial public key validation of the peer EC public key, complying with Section 5.6.2.2.2 of SP 800-56Ar3. The module is compliant to IG D.F scenario 2 path (1).

2.7.5 SHA3

The module provides SHA-3 hash functions compliant with IG C.C. Every implementation of each SHA-3 function was tested and validated on all of the module's operating environments.

SHAKE functions are not implemented.

SHA-3 hash functions are also used as part of a higher-level algorithm for HMAC.

2.7.6 Key Agreement and Key Transport

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

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

2.7.7 SHA-1

The SHA-1 algorithm is currently deprecated and will be non-approved for all purposes, starting January 1, 2031. The module doesn't offer signature generation with SHA-1 in approved mode. Usage of SHA-1 is only approved when used for Message Authentication HMAC, Message Digest, ANS X9.42 Key Derivation, SSH Key Derivation, and Signature Verification (Legacy).

2.8 RBG and Entropy

Cert Number	Vendor Name
E61	Oracle Corp

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
UEK7 CPU Time Jitter RNG Entropy Source	Non-Physical	See Table 2	64	59.41 bits	LFSR

Table 11: Entropy Sources

RNG Information:

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

Additionally, the module employs a specific HMAC SHA-512 DRBG implementation for internal purposes (e.g. to generate asymmetric key pairs or initialization vectors). This DRBG is initially seeded with 448 output bits from the entropy source (415 bits of entropy) and reseeded with 320 output bits from the entropy source (297 bits of entropy).

2.9 Key Generation

The key generation methods implemented by the module are specified in the Vendor-Affirmed Algorithms table. The key derivation methods implemented by the module are specified in the Security Function Implementations table.

2.10 Key Establishment

Key Establishment methods are specified in the Security Function Implementations table.

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API data input parameters
N/A	Data Output	API output parameters
N/A	Control Input	API function calls, API control input parameters
N/A	Status Output	API return codes, error queue

Table 12: Ports and Interfaces

The logical interfaces are the APIs through which the applications request services. These logical interfaces are logically separated from each other by the API design.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement authentication.

4.2 Roles

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

Table 13: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Digest	Compute a message digest	crypto_shash_init returns 0	message	digest value	Hashing	Crypto Officer
Encryption	Encrypt a plaintext	crypto_skcipher_setkey returns 0	AES key, plaintext	Ciphertext	Encryption	Crypto Officer - AES key: W,E
Decryption	Decrypt a ciphertext	crypto_skcipher_setkey returns 0	AES key, ciphertext	Plaintext	Decryption	Crypto Officer - AES key: W,E
Authenticated encryption	Encrypt a plaintext	For all modes except AES GCM: crypto_aead_setkey returns 0 For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	AES key, plaintext	Ciphertext	Authenticated Encryption	Crypto Officer - AES key: W,E - HMAC key: W,E
Authenticated decryption	Decrypt a ciphertext	For all modes except AES GCM: crypto_aead_setkey returns 0 For AES GCM: crypto_aead_get_flags(tfm) has the CRYPTO_TFM_FIPS_COMPLIANCE flag set	AES key, ciphertext	Plaintext	Authenticated Decryption	Crypto Officer - AES key: W,E - HMAC key: W,E
Message authentication	Compute a MAC tag	crypto_shash_init returns 0	AES key, message; HMAC key, message	MAC tag	Message Authentication	Crypto Officer - AES key: W,E - HMAC key: W,E
Shared secret computation	Compute a shared secret	crypto_kpp_compute_shared_secret returns 0	DH private key, DH public key;EC private key, EC	Shared secret	Shared Secret Computation	Crypto Officer - DH public key: W,E - DH private key: W,E - Shared secret: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			public key			- EC public key: W,E - EC private key: W,E - EC SP 800-56Arev3 Domain Parameters: E - DH SP 800-56Arev3 Domain Parameters: E
Key pair generation	Generate a key pair	crypto_kpp_set_secret and crypto_kpp_generate_public_key return 0	Group; Curve	DH private key, DH EC private key, EC public key key;	Key Generation	Crypto Officer - DH public key: G,R - DH private key: G,R - Intermediate Key Generation Value: G,Z - EC public key: G,R - EC private key: G,R
Random number generation	Generate random bytes	crypto_rng_get_bytes returns 0	Output length	Random bytes	Random Numbers	Crypto Officer - CTR_DRBG seed (IG D.L): W,E - Hash_DRBG Seed (IG D.L): G,E - HMAC_DRBG Seed (IG D.L): G,E - Entropy input (IG D.L): E - HMAC_DRBG Internal State (V, Key) (IG D.L): G,E - CTR_DRBG Internal state (V, Key) (IG D.L): G,E - Hash_DRBG Internal State (V, C) (IG D.L): G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Error detection code	Compute an EDC (crc32, crct10dif)	None	Message	EDC	None	Unauthenticated
Compression	Compress data (deflate, lz4, lz4hc, lzo, zlib-deflate, zstd)	None	Data	Compressed data	None	Unauthenticated
Generic system call	Use the kernel to perform various non-cryptographic operations	None	Identifier, various arguments	Various return values	None	Unauthenticated
Show version	Return the module name and version information	None	N/A	Module name and version	None	Unauthenticated
Show status	Return the module status	None	N/A	Module status	None	Unauthenticated
Self-test	Perform the CASTs and integrity tests	None	N/A	Pass/fail	Shared Secret Computation Authenticated Encryption with AES-CBC or AES-CTR with HMAC Authenticated Decryption with AES-CBC or AES-CTR with HMAC Hashing Encryption Decryption Authenticated Encryption Authenticated Decryption Message Authentication Key Generation	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Random Numbers	
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Crypto Officer - AES key: Z - HMAC key: Z - Shared secret: Z - CTR_DRBG seed (IG D.L): Z - Hash_DRBG Seed (IG D.L): Z - HMAC_DRBG Seed (IG D.L): Z - Intermediate Key Generation Value: Z - DH public key: Z - DH private key: Z - EC public key: Z - EC private key: Z - CTR_DRBG Internal state (V, Key) (IG D.L): Z - HMAC_DRBG Internal State (V, Key) (IG D.L): Z - Hash_DRBG Internal State (V, C) (IG D.L): Z - Entropy input (IG D.L): Z
RSA Signature Verification	Verify a digital signature	crypto_akcipher_init returns 0	Signature, RSA public key	Digital signature verification result	RSA Signature Verification (Legacy)	Crypto Officer - RSA public key: W,E

Table 14: Approved Services

For each service, a service indicator is provided by the successful execution of the service (i.e. return value is equal to 0 for the relevant API function) for all cryptographic services, with the exception of AES GCM. For authenticated encryption and decryption using AES GCM, the operator must verify the cipher handle has the CRYPTO_TFM_FIPS_COMPLIANCE set, by using the crypto_aead_get_flags(tfm) API function. If this flag is set, the service is approved.

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

- **Generate (G)**: The module generates or derives the SSP.

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

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES GCM external IV encryption	Encrypt a plaintext using AES GCM with an external IV	AES GCM with external IV	Crypto Officer
Key derivation	Derive a key from a key-derivation key or a shared secret	KBKDF (libkcapi) HKDF (libkcapi)	Crypto Officer
Password-based key derivation	Derive a key from a password	PBKDF2 (libkcapi)	Crypto Officer
RSA encryption primitive	Compute the raw RSA encryption of a plaintext/ciphertext	RSA	Crypto Officer
RSA decryption primitive	Compute the raw RSA decryption of a plaintext/ciphertext	RSA	Crypto Officer
RSA signature generation (pre-hashed message)	Generate a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	Crypto Officer
RSA signature verification (pre-hashed message)	Verify a digital signature for a pre-hashed message	RSA with PKCS#1 v1.5 padding	Crypto Officer
Key encapsulation	Encapsulate a secret key using RSA with PKCS#1 v1.5 padding	RSA with PKCS#1 v1.5 padding	Crypto Officer
Key decapsulation	Decapsulate a secret key using RSA with PKCS#1 v1.5 padding	RSA with PKCS#1 v1.5 padding	Crypto Officer
ECDSA signature verification primitive	Verify ECDSA-based signatures	ECDSA Signature Verification Primitive	Crypto Officer

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The Linux kernel binary is integrity tested using an HMAC SHA-512 calculation performed by the sha512hmac utility (which utilizes the module's HMAC and SHA-512 implementations) which compares the computed HMAC value with a precomputed HMAC value. An HMAC SHA-512 calculation is also performed on the sha512hmac utility and the libkcapi library to verify their integrity by comparing the computed HMAC value with a precomputed HMAC value. The kernel crypto object files listed in the Executable Code Sets Table are loaded on start-up by the module and verified using RSA signature verification with PKCS#1 v1.5 padding, SHA-512, and a 4096-bit key.

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

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

6.2 Configuration Settings and Restrictions

The module shall be installed as stated in Section 11.1.

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

7 Physical Security

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 16: Storage Areas

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

9.2 SSP Input-Output Methods

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

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

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

Table 18: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for Encryption;	128, 192, 256 bits - 128, 192, 256 bits	CSP - CSP			Authenticated Encryption with

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Decryption; Authenticated encryption; Authenticated decryption; Message authentication					AES-CBC or AES-CTR with HMAC Authenticated Decryption with AES-CBC or AES-CTR with HMAC Encryption Decryption Authenticated Encryption Authenticated Decryption Message Authentication
HMAC key	HMAC key used for Message authentication code (MAC)	112-256 bits - 112-256 bits	CSP - CSP			Message Authentication
Shared secret	Shared secret established during Shared Secret Computation	EC Diffie-Hellman 256 and 384; Diffie-Hellman 2048-8192 bits - EC Diffie-Hellman 128 and 192; Diffie-Hellman 112-200 bits	CSP - CSP		Shared Secret Computation	
CTR_DRBG seed (IG D.L)	DRBG seed derived from Entropy Input	256, 320, 384 bits - 128, 192, 256 bits	CSP - CSP	Random Numbers		Random Numbers
Hash_DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	440, 888 bits - 128, 256 bits	CSP - CSP	Random Numbers		Random Numbers
HMAC_DRBG Seed (IG D.L)	DRBG seed derived from Entropy Input	440, 888 bits - 128, 256 bits	CSP - CSP	Random Numbers		Random Numbers
Entropy input (IG D.L)	Entropy input used to seed the DRBGs	128-384 bits - 128-256 bits	CSP - CSP			Random Numbers
CTR_DRBG Internal state (V, Key) (IG D.L)	Internal state of CTR_DRBG instance	256, 320, 384 bits - 128, 192, 256 bits	CSP - CSP	Random Numbers		Random Numbers
HMAC_DRBG Internal State (V, Key) (IG D.L)	Internal state of HMAC DRBG instance	320, 512, 1024 bits - 128, 256 bits	CSP - CSP	Random Numbers		Random Numbers
Hash_DRBG Internal State (V, C) (IG D.L)	Internal state of Hash DRBG instance	880, 1776 bits - 128, 256 bits	CSP - CSP	Random Numbers		Random Numbers
Intermediate Key Generation Value	intermediate value	fdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, P-256, P-384 (112- 200 bits) -	CSP - CSP	Key Generation		Key Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		fdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, P-256, P-384 (112- 200 bits)				
DH public key	DH public key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112- 200 bits) - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112- 200 bits)	PSP - PSP	Key Generation		
DH private key	DH private key used for KAS-FFC-SSC	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112- 200 bits) - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (112- 200 bits)	CSP - CSP	Key Generation		
EC public key	Public key used for KAS-ECC-SSC	P-256, P-384 (256, 384 bits) - P-256, P-384 (128, 192 bits)	PSP - PSP	Key Generation		
EC private key	EC private key used for KAS-ECC-SSC	P-256, P-384 (256, 384 bits) - P-256, P-384 (128, 192 bits)	CSP - CSP	Key Generation		
RSA public key	Public key used for RSA Signature Verification	2048, 3072, or 4096-bits - 112-150 bits	PSP - CSP			RSA Signature Verification (Legacy)
EC SP 800-56Arev3 Domain Parameters	Domain parameters used for KAS-ECC-SSC	P-256, P-384 (1536, 2304 bits) - N/A	PSP - PSP			Shared Secret Computation
DH SP 800-56Arev3 Domain Parameters	Domain parameters used for KAS-ECC-SSC	fdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (2056-8200 bits) - N/A	PSP - PSP			Shared Secret Computation

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext		Free cipher handle Remove power from the module	
HMAC key	API input parameters; AF_ALG_type sockets (input)	RAM:Plaintext		Free cipher handle Remove power from the module	
Shared secret	API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Free cipher handle Remove power from the module	DH public key:Derived From DH private key:Derived From EC public key:Derived From EC private key:Derived From EC SP 800-56Arev3 Domain Parameters:Derived From DH SP 800-56Arev3 Domain Parameters:Derived From
CTR_DRBG seed (IG D.L)		RAM:Plaintext		Remove power from the module Automatic	Entropy input (IG D.L):Derived From CTR_DRBG Internal state (V, Key) (IG D.L):Derives
Hash_DRBG Seed (IG D.L)		RAM:Plaintext		Remove power from the module Automatic	Entropy input (IG D.L):Derived From Hash_DRBG Internal State (V, C) (IG D.L):Derives
HMAC_DRBG Seed (IG D.L)		RAM:Plaintext		Remove power from the module Automatic	Entropy input (IG D.L):Derived From HMAC_DRBG Internal State (V, Key) (IG D.L):Derives
Entropy input (IG D.L)		RAM:Plaintext		Remove power from the module Automatic	CTR_DRBG seed (IG D.L):Derives Hash_DRBG Seed (IG D.L):Derives HMAC_DRBG Seed (IG D.L):Derives
CTR_DRBG Internal state (V, Key) (IG D.L)		RAM:Plaintext		Free cipher handle Remove power from the module	CTR_DRBG Internal state (V, Key) (IG D.L):Derived From
HMAC_DRBG Internal State (V, Key) (IG D.L)		RAM:Plaintext		Free cipher handle Remove power from the module	HMAC_DRBG Internal State (V, Key) (IG D.L):Derived From
Hash_DRBG Internal State (V, C) (IG D.L)		RAM:Plaintext		Free cipher handle Remove power	Hash_DRBG Seed (IG D.L):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				from the module	
Intermediate Key Generation Value		RAM:Plaintext		Automatic	DH public key:Generates DH private key:Generates EC public key:Generates EC private key:Generates
DH public key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Free cipher handle Remove power from the module	DH private key:Paired With Intermediate Key Generation Value:Generated From
DH private key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Free cipher handle Remove power from the module	DH public key:Paired With Intermediate Key Generation Value:Generated From
EC public key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Free cipher handle Remove power from the module	EC private key:Paired With Intermediate Key Generation Value:Generated From
EC private key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Free cipher handle Remove power from the module	EC public key:Paired With Intermediate Key Generation Value:Generated From
RSA public key	API input parameters; AF_ALG_type sockets (input) API output parameters; AF_ALG type sockets (output)	RAM:Plaintext		Remove power from the module Automatic	
EC SP 800-56Arev3 Domain Parameters		RAM:Plaintext		Free cipher handle Remove power from the module	EC public key:Used With EC private key:Used With Shared secret:Derives
DH SP 800-56Arev3 Domain Parameters		RAM:Plaintext		Free cipher handle Remove power from the module	DH public key:Used With DH private key:Used With Shared secret:Derives

Table 20: SSP Table 2

9.5 Transitions

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-512 (A3887) (OL8 Intel and AMD)	512-bit key	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
HMAC-SHA2-512 (A3890) (OL8 Ampere)	512-bit key	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
RSA SigVer (FIPS186-4) (A3887) (OL8 Intel and AMD)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational	Integrity test for kernel object files
RSA SigVer (FIPS186-4) (A3862) (OL8 Ampere)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational	Integrity test for kernel object files
HMAC-SHA2-512 (A4192) (OL9 Intel and AMD)	512-bit key	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
HMAC-SHA2-512 (A4177) (OL9 Ampere)	512-bit key	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
HMAC-SHA2-512 (A4162) (OL9 Marvell)	512-bit key	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for vmlinuz, libkcapi components and sha512hmac binary
RSA SigVer (FIPS186-4) (A4192) (OL9 Intel and AMD)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational	Integrity test for kernel object files
RSA SigVer (FIPS186-4) (A4162) (OL9 Marvell and Ampere)	4096-bit key with SHA-512	Signature Verification	SW/FW Integrity	Module becomes operational	Integrity test for kernel object files

Table 21: Pre-Operational Self-Tests

The pre-operational software integrity tests are performed automatically when the module is powered on, before the module transitions into the operational state. The algorithms used for the integrity test (i.e., HMAC-SHA2-512 and RSA SigVer with 4096 bit key) run their CASTs before the integrity test is performed. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the pre-operational software integrity self-tests are successfully completed. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-CBC (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A3894)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4179)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC-CS3 (A3866)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A3874)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A3884)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (4166)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A4174)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CBC-CS3 (A4188)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-CCM (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CCM (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A3864)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A3872)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A3882)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A4164)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB128 (A4172)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CFB128 (A4186)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CMAC (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-CTR (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A3894)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4179)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-CTR (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3860)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3861)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3867)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3868)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3870)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3871)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3877)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3878)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-ECB (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3880)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3881)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3892)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3893)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A3894)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4160)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4161)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4167)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A4168)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4170)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4171)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4179)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4181)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4182)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4184)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4185)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-ECB (A4196)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-ECB (A4197)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3867)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3868)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3870)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3871)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3877)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3878)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A3880)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3881)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3892)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A3893)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4167)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4168)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4170)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4171)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4181)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-GCM (A4182)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4184)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4185)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4196)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-GCM (A4197)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A3865)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A3873)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A3883)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A4165)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-OFB (A4173)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-OFB (A4187)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3889)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A3894)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (A4176)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4179)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
AES-XTS Testing Revision 2.0 (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Symmetric operation	Module initialization
ECDSA KeyGen (FIPS186-4) (A3861)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4161)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
Counter DRBG (A3860)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3861)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3862)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3867)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3868)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3869)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A3870)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3871)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3876)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3877)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3878)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3879)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3880)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3881)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3891)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3892)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A3893)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4160)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4161)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
Counter DRBG (A4162)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4167)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4168)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4169)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4170)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4171)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4178)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4181)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4182)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4183)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4184)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4185)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A4191)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4196)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Counter DRBG (A4197)	128, 192, 256-bit key	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3860)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3861)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3862)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3867)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3868)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3869)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3870)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3871)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3876)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3877)	SHA2-256	KAT	CAST	Module becomes operational and	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
Hash DRBG (A3878)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3879)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3880)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3881)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3885)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3886)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3887)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3891)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3892)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A3893)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4160)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4161)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A4162)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4167)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4168)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4169)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4170)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4171)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4181)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4182)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4183)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4184)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4185)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4189)	SHA2-256	KAT	CAST	Module becomes operational and	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
Hash DRBG (A4190)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4191)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4192)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4196)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
Hash DRBG (A4197)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3860)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3861)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3862)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3867)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3868)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3869)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3870)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A3871)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3876)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3877)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3878)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3879)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3880)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3881)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3885)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3886)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3887)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3891)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3892)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A3893)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC DRBG (A4160)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4161)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4162)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4167)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4168)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4169)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4170)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4171)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4181)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4182)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4183)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A4184)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4185)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4189)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4190)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4191)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4192)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4196)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC DRBG (A4197)	SHA2-256, SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Seed Generate	Module initialization
HMAC-SHA-1 (A3860)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3861)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3862)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3885)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3886)	SHA-1	KAT	CAST	Module becomes operational and	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC-SHA-1 (A3887)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3888)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A3889)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4160)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4161)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4162)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4176)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4189)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4190)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4192)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A4193)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA-1 (A6709)	SHA-1	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A3860)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3861)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3862)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3885)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3886)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3887)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3888)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3889)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3894)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A3895)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4160)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4161)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4162)	SHA2-224	KAT	CAST	Module becomes operational and	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC-SHA2-224 (A4176)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4179)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4180)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4189)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4190)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4192)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A4193)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-224 (A6709)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3860)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3861)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3862)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3885)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A3886)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3887)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3888)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3889)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3894)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A3895)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4160)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4161)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4162)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4176)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4179)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4180)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4189)	SHA2-256	KAT	CAST	Module becomes operational and	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC-SHA2-256 (A4190)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4192)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A4193)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-256 (A6709)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3860)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3861)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3862)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3885)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3886)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3887)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3888)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3889)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A3890)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A3895)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4160)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4161)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4162)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4176)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4177)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4180)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4189)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4190)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4192)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A4193)	SHA2-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-384 (A6709)	SHA2-384	KAT	CAST	Module becomes operational and	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC-SHA2-512 (A3860)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3861)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3862)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3885)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3886)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3887)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3888)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3889)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3890)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A3895)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4160)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4161)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A4162)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4176)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4177)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4180)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4189)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4190)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4192)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A4193)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA2-512 (A6709)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-224 (A3863)	SHA3-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-224 (A4163)	SHA3-224	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-256 (A3863)	SHA3-256	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-256 (A4163)	SHA3-256	KAT	CAST	Module becomes operational and	Message authentication	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
HMAC-SHA3-384 (A3863)	SHA3-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-384 (A4163)	SHA3-384	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-512 (A3863)	SHA3-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
HMAC-SHA3-512 (A4163)	SHA3-512	KAT	CAST	Module becomes operational and services are available for use	Message authentication	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A3861)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A4161)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
KAS-FFC-SSC Sp800-56Ar3 (A3860)	MODP-2048	PCT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
KAS-FFC-SSC Sp800-56Ar3 (A4160)	MODP-2048	PCT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Module initialization
Safe Primes Key Generation (A3860)	Section 5.6.2.1.4 of SP800-56Arev3	PCT	PCT	Module becomes operational and services are available for use.	SP 800-56ARev3, 5.6.2.1.4	Module initialization
Safe Primes Key Generation (A4160)	Section 5.6.2.1.4 of SP800-56Arev3	PCT	PCT	Module becomes operational and services are available for use.	SP 800-56ARev3, 5.6.2.1.4	Module initialization
SHA-1 (A3860)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3861)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A3862)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3885)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3886)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3887)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3888)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A3889)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4160)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4161)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4162)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4176)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4189)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4190)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A4192)	message	KAT	CAST	Module becomes operational and	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use.		
SHA-1 (A4193)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA-1 (A6709)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3860)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3861)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3862)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3885)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3886)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3887)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3888)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3889)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3894)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A3895)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-224 (A4160)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4161)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4162)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4176)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4179)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4180)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4189)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4190)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4192)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A4193)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-224 (A6709)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3860)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3861)	message	KAT	CAST	Module becomes operational and	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use.		
SHA2-256 (A3862)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3885)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3886)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3887)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3888)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3889)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3894)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A3895)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4160)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4161)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4162)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4176)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A4179)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4180)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4189)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4190)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4192)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A4193)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-256 (A6709)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3860)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3861)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3862)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3885)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3886)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3887)	message	KAT	CAST	Module becomes operational and	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use.		
SHA2-384 (A3888)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3889)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3890)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A3895)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4160)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4161)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4162)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4176)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4177)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4180)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4189)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4190)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A4192)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A4193)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-384 (A6709)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3860)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3861)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3862)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3885)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3886)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3887)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3888)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3889)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3890)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A3895)	message	KAT	CAST	Module becomes operational and	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use.		
SHA2-512 (A4160)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4161)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4162)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4176)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4177)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4180)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4189)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4190)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4192)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A4193)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA2-512 (A6709)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-224 (A3863)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA3-224 (A4163)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-256 (A3863)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-256 (A4163)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-384 (A3863)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-384 (A4163)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-512 (A3863)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
SHA3-512 (A4163)	message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Module initialization
RSA SigVer (FIPS186-4) (A4162)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4189)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4190)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4192)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3862)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3885)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A3886)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A3887)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Table 22: Conditional Self-Tests

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

Upon generation of a DH or EC key pair, the module will perform a pair-wise consistency test (PCT) as shown in the Conditional Self-Tests Table, which provides some assurance that the generated key pair is well formed. This test consists of the PCT described in Section 5.6.2.1.4 of SP 800-56Ar3. Services are not available, and data output (via the data output interface) is inhibited during execution of the PCT. If the test 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-SHA2-512 (A3887) (OL8 Intel and AMD)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-512 (A3890) (OL8 Ampere)	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-4) (A3887) (OL8 Intel and AMD)	Signature Verification	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-4) (A3862) (OL8 Ampere)	Signature Verification	SW/FW Integrity	On demand	Manually
HMAC-SHA2-512 (A4192) (OL9 Intel and AMD)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-512 (A4177) (OL9 Ampere)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-512 (A4162) (OL9 Marvell)	Message Authentication	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-4) (A4192) (OL9 Intel and AMD)	Signature Verification	SW/FW Integrity	On demand	Manually
RSA SigVer (FIPS186-4) (A4162) (OL9 Marvell and Ampere)	Signature Verification	SW/FW Integrity	On demand	Manually

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3862)	KAT	CAST	On Demand	Manually
AES-CBC (A3869)	KAT	CAST	On Demand	Manually
AES-CBC (A3876)	KAT	CAST	On Demand	Manually
AES-CBC (A3879)	KAT	CAST	On Demand	Manually
AES-CBC (A3889)	KAT	CAST	On Demand	Manually
AES-CBC (A3891)	KAT	CAST	On Demand	Manually
AES-CBC (A3894)	KAT	CAST	On Demand	Manually
AES-CBC (A4162)	KAT	CAST	On Demand	Manually
AES-CBC (A4169)	KAT	CAST	On Demand	Manually
AES-CBC (A4176)	KAT	CAST	On Demand	Manually
AES-CBC (A4178)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A4179)	KAT	CAST	On Demand	Manually
AES-CBC (A4183)	KAT	CAST	On Demand	Manually
AES-CBC (A4191)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3866)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3874)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3884)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3889)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A3891)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (4166)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A4174)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A4176)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A4178)	KAT	CAST	On Demand	Manually
AES-CBC-CS3 (A4188)	KAT	CAST	On Demand	Manually
AES-CCM (A3862)	KAT	CAST	On Demand	Manually
AES-CCM (A3869)	KAT	CAST	On Demand	Manually
AES-CCM (A3879)	KAT	CAST	On Demand	Manually
AES-CCM (A3889)	KAT	CAST	On Demand	Manually
AES-CCM (A3891)	KAT	CAST	On Demand	Manually
AES-CCM (A4162)	KAT	CAST	On Demand	Manually
AES-CCM (A4169)	KAT	CAST	On Demand	Manually
AES-CCM (A4176)	KAT	CAST	On Demand	Manually
AES-CCM (A4178)	KAT	CAST	On Demand	Manually
AES-CCM (A4183)	KAT	CAST	On Demand	Manually
AES-CFB128 (A3864)	KAT	CAST	On Demand	Manually
AES-CFB128 (A3872)	KAT	CAST	On Demand	Manually
AES-CFB128 (A3882)	KAT	CAST	On Demand	Manually
AES-CFB128 (A3891)	KAT	CAST	On Demand	Manually
AES-CFB128 (A4164)	KAT	CAST	On Demand	Manually
AES-CFB128 (A4172)	KAT	CAST	On Demand	Manually
AES-CFB128 (A4178)	KAT	CAST	On Demand	Manually
AES-CFB128 (A4186)	KAT	CAST	On Demand	Manually
AES-CMAC (A3862)	KAT	CAST	On Demand	Manually
AES-CMAC (A3869)	KAT	CAST	On Demand	Manually
AES-CMAC (A3879)	KAT	CAST	On Demand	Manually
AES-CMAC (A3889)	KAT	CAST	On Demand	Manually
AES-CMAC (A3891)	KAT	CAST	On Demand	Manually
AES-CMAC (A4162)	KAT	CAST	On Demand	Manually
AES-CMAC (A4169)	KAT	CAST	On Demand	Manually
AES-CMAC (A4176)	KAT	CAST	On Demand	Manually
AES-CMAC (A4178)	KAT	CAST	On Demand	Manually
AES-CMAC (A4183)	KAT	CAST	On Demand	Manually
AES-CTR (A3862)	KAT	CAST	On Demand	Manually
AES-CTR (A3869)	KAT	CAST	On Demand	Manually
AES-CTR (A3876)	KAT	CAST	On Demand	Manually
AES-CTR (A3879)	KAT	CAST	On Demand	Manually
AES-CTR (A3889)	KAT	CAST	On Demand	Manually
AES-CTR (A3891)	KAT	CAST	On Demand	Manually
AES-CTR (A3894)	KAT	CAST	On Demand	Manually
AES-CTR (A4162)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (A4169)	KAT	CAST	On Demand	Manually
AES-CTR (A4176)	KAT	CAST	On Demand	Manually
AES-CTR (A4178)	KAT	CAST	On Demand	Manually
AES-CTR (A4179)	KAT	CAST	On Demand	Manually
AES-CTR (A4183)	KAT	CAST	On Demand	Manually
AES-CTR (A4191)	KAT	CAST	On Demand	Manually
AES-ECB (A3860)	KAT	CAST	On Demand	Manually
AES-ECB (A3861)	KAT	CAST	On Demand	Manually
AES-ECB (A3862)	KAT	CAST	On Demand	Manually
AES-ECB (A3867)	KAT	CAST	On Demand	Manually
AES-ECB (A3868)	KAT	CAST	On Demand	Manually
AES-ECB (A3869)	KAT	CAST	On Demand	Manually
AES-ECB (A3870)	KAT	CAST	On Demand	Manually
AES-ECB (A3871)	KAT	CAST	On Demand	Manually
AES-ECB (A3876)	KAT	CAST	On Demand	Manually
AES-ECB (A3877)	KAT	CAST	On Demand	Manually
AES-ECB (A3878)	KAT	CAST	On Demand	Manually
AES-ECB (A3879)	KAT	CAST	On Demand	Manually
AES-ECB (A3880)	KAT	CAST	On Demand	Manually
AES-ECB (A3881)	KAT	CAST	On Demand	Manually
AES-ECB (A3889)	KAT	CAST	On Demand	Manually
AES-ECB (A3891)	KAT	CAST	On Demand	Manually
AES-ECB (A3892)	KAT	CAST	On Demand	Manually
AES-ECB (A3893)	KAT	CAST	On Demand	Manually
AES-ECB (A3894)	KAT	CAST	On Demand	Manually
AES-ECB (A4160)	KAT	CAST	On Demand	Manually
AES-ECB (A4161)	KAT	CAST	On Demand	Manually
AES-ECB (A4162)	KAT	CAST	On Demand	Manually
AES-ECB (A4167)	KAT	CAST	On Demand	Manually
AES-ECB (A4168)	KAT	CAST	On Demand	Manually
AES-ECB (A4169)	KAT	CAST	On Demand	Manually
AES-ECB (A4170)	KAT	CAST	On Demand	Manually
AES-ECB (A4171)	KAT	CAST	On Demand	Manually
AES-ECB (A4176)	KAT	CAST	On Demand	Manually
AES-ECB (A4178)	KAT	CAST	On Demand	Manually
AES-ECB (A4179)	KAT	CAST	On Demand	Manually
AES-ECB (A4181)	KAT	CAST	On Demand	Manually
AES-ECB (A4182)	KAT	CAST	On Demand	Manually
AES-ECB (A4183)	KAT	CAST	On Demand	Manually
AES-ECB (A4184)	KAT	CAST	On Demand	Manually
AES-ECB (A4185)	KAT	CAST	On Demand	Manually
AES-ECB (A4191)	KAT	CAST	On Demand	Manually
AES-ECB (A4196)	KAT	CAST	On Demand	Manually
AES-ECB (A4197)	KAT	CAST	On Demand	Manually
AES-GCM (A3862)	KAT	CAST	On Demand	Manually
AES-GCM (A3867)	KAT	CAST	On Demand	Manually
AES-GCM (A3868)	KAT	CAST	On Demand	Manually
AES-GCM (A3869)	KAT	CAST	On Demand	Manually
AES-GCM (A3870)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3871)	KAT	CAST	On Demand	Manually
AES-GCM (A3876)	KAT	CAST	On Demand	Manually
AES-GCM (A3877)	KAT	CAST	On Demand	Manually
AES-GCM (A3878)	KAT	CAST	On Demand	Manually
AES-GCM (A3879)	KAT	CAST	On Demand	Manually
AES-GCM (A3880)	KAT	CAST	On Demand	Manually
AES-GCM (A3881)	KAT	CAST	On Demand	Manually
AES-GCM (A3891)	KAT	CAST	On Demand	Manually
AES-GCM (A3892)	KAT	CAST	On Demand	Manually
AES-GCM (A3893)	KAT	CAST	On Demand	Manually
AES-GCM (A4162)	KAT	CAST	On Demand	Manually
AES-GCM (A4167)	KAT	CAST	On Demand	Manually
AES-GCM (A4168)	KAT	CAST	On Demand	Manually
AES-GCM (A4169)	KAT	CAST	On Demand	Manually
AES-GCM (A4170)	KAT	CAST	On Demand	Manually
AES-GCM (A4171)	KAT	CAST	On Demand	Manually
AES-GCM (A4178)	KAT	CAST	On Demand	Manually
AES-GCM (A4181)	KAT	CAST	On Demand	Manually
AES-GCM (A4182)	KAT	CAST	On Demand	Manually
AES-GCM (A4183)	KAT	CAST	On Demand	Manually
AES-GCM (A4184)	KAT	CAST	On Demand	Manually
AES-GCM (A4185)	KAT	CAST	On Demand	Manually
AES-GCM (A4191)	KAT	CAST	On Demand	Manually
AES-GCM (A4196)	KAT	CAST	On Demand	Manually
AES-GCM (A4197)	KAT	CAST	On Demand	Manually
AES-OFB (A3865)	KAT	CAST	On Demand	Manually
AES-OFB (A3873)	KAT	CAST	On Demand	Manually
AES-OFB (A3883)	KAT	CAST	On Demand	Manually
AES-OFB (A3891)	KAT	CAST	On Demand	Manually
AES-OFB (A4165)	KAT	CAST	On Demand	Manually
AES-OFB (A4173)	KAT	CAST	On Demand	Manually
AES-OFB (A4178)	KAT	CAST	On Demand	Manually
AES-OFB (A4187)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3862)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3869)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3876)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3879)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3889)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3891)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A3894)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4162)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4169)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4176)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4178)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4179)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4183)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4191)	KAT	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A3861)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4161)	PCT	PCT	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A3860)	KAT	CAST	On Demand	Manually
Counter DRBG (A3861)	KAT	CAST	On Demand	Manually
Counter DRBG (A3862)	KAT	CAST	On Demand	Manually
Counter DRBG (A3867)	KAT	CAST	On Demand	Manually
Counter DRBG (A3868)	KAT	CAST	On Demand	Manually
Counter DRBG (A3869)	KAT	CAST	On Demand	Manually
Counter DRBG (A3870)	KAT	CAST	On Demand	Manually
Counter DRBG (A3871)	KAT	CAST	On Demand	Manually
Counter DRBG (A3876)	KAT	CAST	On Demand	Manually
Counter DRBG (A3877)	KAT	CAST	On Demand	Manually
Counter DRBG (A3878)	KAT	CAST	On Demand	Manually
Counter DRBG (A3879)	KAT	CAST	On Demand	Manually
Counter DRBG (A3880)	KAT	CAST	On Demand	Manually
Counter DRBG (A3881)	KAT	CAST	On Demand	Manually
Counter DRBG (A3891)	KAT	CAST	On Demand	Manually
Counter DRBG (A3892)	KAT	CAST	On Demand	Manually
Counter DRBG (A3893)	KAT	CAST	On Demand	Manually
Counter DRBG (A4160)	KAT	CAST	On Demand	Manually
Counter DRBG (A4161)	KAT	CAST	On Demand	Manually
Counter DRBG (A4162)	KAT	CAST	On Demand	Manually
Counter DRBG (A4167)	KAT	CAST	On Demand	Manually
Counter DRBG (A4168)	KAT	CAST	On Demand	Manually
Counter DRBG (A4169)	KAT	CAST	On Demand	Manually
Counter DRBG (A4170)	KAT	CAST	On Demand	Manually
Counter DRBG (A4171)	KAT	CAST	On Demand	Manually
Counter DRBG (A4178)	KAT	CAST	On Demand	Manually
Counter DRBG (A4181)	KAT	CAST	On Demand	Manually
Counter DRBG (A4182)	KAT	CAST	On Demand	Manually
Counter DRBG (A4183)	KAT	CAST	On Demand	Manually
Counter DRBG (A4184)	KAT	CAST	On Demand	Manually
Counter DRBG (A4185)	KAT	CAST	On Demand	Manually
Counter DRBG (A4191)	KAT	CAST	On Demand	Manually
Counter DRBG (A4196)	KAT	CAST	On Demand	Manually
Counter DRBG (A4197)	KAT	CAST	On Demand	Manually
Hash DRBG (A3860)	KAT	CAST	On Demand	Manually
Hash DRBG (A3861)	KAT	CAST	On Demand	Manually
Hash DRBG (A3862)	KAT	CAST	On Demand	Manually
Hash DRBG (A3867)	KAT	CAST	On Demand	Manually
Hash DRBG (A3868)	KAT	CAST	On Demand	Manually
Hash DRBG (A3869)	KAT	CAST	On Demand	Manually
Hash DRBG (A3870)	KAT	CAST	On Demand	Manually
Hash DRBG (A3871)	KAT	CAST	On Demand	Manually
Hash DRBG (A3876)	KAT	CAST	On Demand	Manually
Hash DRBG (A3877)	KAT	CAST	On Demand	Manually
Hash DRBG (A3878)	KAT	CAST	On Demand	Manually
Hash DRBG (A3879)	KAT	CAST	On Demand	Manually
Hash DRBG (A3880)	KAT	CAST	On Demand	Manually
Hash DRBG (A3881)	KAT	CAST	On Demand	Manually
Hash DRBG (A3885)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A3886)	KAT	CAST	On Demand	Manually
Hash DRBG (A3887)	KAT	CAST	On Demand	Manually
Hash DRBG (A3891)	KAT	CAST	On Demand	Manually
Hash DRBG (A3892)	KAT	CAST	On Demand	Manually
Hash DRBG (A3893)	KAT	CAST	On Demand	Manually
Hash DRBG (A4160)	KAT	CAST	On Demand	Manually
Hash DRBG (A4161)	KAT	CAST	On Demand	Manually
Hash DRBG (A4162)	KAT	CAST	On Demand	Manually
Hash DRBG (A4167)	KAT	CAST	On Demand	Manually
Hash DRBG (A4168)	KAT	CAST	On Demand	Manually
Hash DRBG (A4169)	KAT	CAST	On Demand	Manually
Hash DRBG (A4170)	KAT	CAST	On Demand	Manually
Hash DRBG (A4171)	KAT	CAST	On Demand	Manually
Hash DRBG	KAT	CAST	On Demand	Manually
Hash DRBG (A4181)	KAT	CAST	On Demand	Manually
Hash DRBG (A4182)	KAT	CAST	On Demand	Manually
Hash DRBG (A4183)	KAT	CAST	On Demand	Manually
Hash DRBG (A4184)	KAT	CAST	On Demand	Manually
Hash DRBG (A4185)	KAT	CAST	On Demand	Manually
Hash DRBG (A4189)	KAT	CAST	On Demand	Manually
Hash DRBG (A4190)	KAT	CAST	On Demand	Manually
Hash DRBG (A4191)	KAT	CAST	On Demand	Manually
Hash DRBG (A4192)	KAT	CAST	On Demand	Manually
Hash DRBG (A4196)	KAT	CAST	On Demand	Manually
Hash DRBG (A4197)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3860)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3861)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3862)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3867)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3868)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3869)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3870)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3871)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3876)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3877)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3878)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3879)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3880)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3881)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3885)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3886)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3887)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3891)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3892)	KAT	CAST	On Demand	Manually
HMAC DRBG (A3893)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4160)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4161)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4162)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4167)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC DRBG (A4168)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4169)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4170)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4171)	KAT	CAST	On Demand	Manually
HMAC DRBG	KAT	CAST	On Demand	Manually
HMAC DRBG (A4181)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4182)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4183)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4184)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4185)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4189)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4190)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4191)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4192)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4196)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4197)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3860)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3861)	KAT	CAST		
HMAC-SHA-1 (A3862)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3885)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3886)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3887)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3888)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A3889)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4160)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4161)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4162)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4176)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4189)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4190)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4192)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4193)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A6709)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3860)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3861)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3862)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3885)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3886)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3887)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3888)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3889)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3894)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A3895)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4160)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4161)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4162)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4176)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4179)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4180)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-224 (A4189)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4190)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4192)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A4193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-224 (A6709)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3860)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3861)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3862)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3885)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3886)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3887)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3888)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3889)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3894)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A3895)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4160)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4161)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4162)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4176)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4179)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4180)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4189)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4190)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4192)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6709)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3860)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3861)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3862)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3885)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3886)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3887)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3888)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3889)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3890)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A3895)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4160)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4161)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4162)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4176)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4177)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4180)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4189)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4190)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4192)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A4193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-384 (A6709)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3860)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3861)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A3862)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3885)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3886)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3887)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3888)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3889)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3890)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A3895)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4160)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4161)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4162)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4176)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4177)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4180)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4189)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4190)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4192)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4193)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A6709)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A3863)	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A4163)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A3863)	KAT	CAST	On Demand	Manually
HMAC-SHA3-256 (A4163)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A3863)	KAT	CAST	On Demand	Manually
HMAC-SHA3-384 (A4163)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A3863)	KAT	CAST	On Demand	Manually
HMAC-SHA3-512 (A4163)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A3861)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4161)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A3860)	PCT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A4160)	PCT	CAST	On Demand	Manually
Safe Primes Key Generation (A3860)	PCT	PCT	On Demand	Manually
Safe Primes Key Generation (A4160)	PCT	PCT	On Demand	Manually
SHA-1 (A3860)	KAT	CAST	On Demand	Manually
SHA-1 (A3861)	KAT	CAST	On Demand	Manually
SHA-1 (A3862)	KAT	CAST	On Demand	Manually
SHA-1 (A3885)	KAT	CAST	On Demand	Manually
SHA-1 (A3886)	KAT	CAST	On Demand	Manually
SHA-1 (A3887)	KAT	CAST	On Demand	Manually
SHA-1 (A3888)	KAT	CAST	On Demand	Manually
SHA-1 (A3889)	KAT	CAST	On Demand	Manually
SHA-1 (A4160)	KAT	CAST	On Demand	Manually
SHA-1 (A4161)	KAT	CAST	On Demand	Manually
SHA-1 (A4162)	KAT	CAST	On Demand	Manually
SHA-1 (A4176)	KAT	CAST	On Demand	Manually
SHA-1 (A4189)	KAT	CAST	On Demand	Manually
SHA-1 (A4190)	KAT	CAST	On Demand	Manually
SHA-1 (A4192)	KAT	CAST	On Demand	Manually
SHA-1 (A4193)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A6709)	KAT	CAST	On Demand	Manually
SHA2-224 (A3860)	KAT	CAST	On Demand	Manually
SHA2-224 (A3861)	KAT	CAST	On Demand	Manually
SHA2-224 (A3862)	KAT	CAST	On Demand	Manually
SHA2-224 (A3885)	KAT	CAST	On Demand	Manually
SHA2-224 (A3886)	KAT	CAST	On Demand	Manually
SHA2-224 (A3887)	KAT	CAST	On Demand	Manually
SHA2-224 (A3888)	KAT	CAST	On Demand	Manually
SHA2-224 (A3889)	KAT	CAST	On Demand	Manually
SHA2-224 (A3894)	KAT	CAST	On Demand	Manually
SHA2-224 (A3895)	KAT	CAST	On Demand	Manually
SHA2-224 (A4160)	KAT	CAST	On Demand	Manually
SHA2-224 (A4161)	KAT	CAST	On Demand	Manually
SHA2-224 (A4162)	KAT	CAST	On Demand	Manually
SHA2-224 (A4176)	KAT	CAST	On Demand	Manually
SHA2-224 (A4179)	KAT	CAST	On Demand	Manually
SHA2-224 (A4180)	KAT	CAST	On Demand	Manually
SHA2-224 (A4189)	KAT	CAST	On Demand	Manually
SHA2-224 (A4190)	KAT	CAST	On Demand	Manually
SHA2-224 (A4192)	KAT	CAST	On Demand	Manually
SHA2-224 (A4193)	KAT	CAST	On Demand	Manually
SHA2-224 (A6709)	KAT	CAST	On Demand	Manually
SHA2-256 (A3860)	KAT	CAST	On Demand	Manually
SHA2-256 (A3861)	KAT	CAST	On Demand	Manually
SHA2-256 (A3862)	KAT	CAST	On Demand	Manually
SHA2-256 (A3885)	KAT	CAST	On Demand	Manually
SHA2-256 (A3886)	KAT	CAST	On Demand	Manually
SHA2-256 (A3887)	KAT	CAST	On Demand	Manually
SHA2-256 (A3888)	KAT	CAST	On Demand	Manually
SHA2-256 (A3889)	KAT	CAST	On Demand	Manually
SHA2-256 (A3894)	KAT	CAST	On Demand	Manually
SHA2-256 (A3895)	KAT	CAST	On Demand	Manually
SHA2-256 (A4160)	KAT	CAST	On Demand	Manually
SHA2-256 (A4161)	KAT	CAST	On Demand	Manually
SHA2-256 (A4162)	KAT	CAST	On Demand	Manually
SHA2-256 (A4176)	KAT	CAST	On Demand	Manually
SHA2-256 (A4179)	KAT	CAST	On Demand	Manually
SHA2-256 (A4180)	KAT	CAST	On Demand	Manually
SHA2-256 (A4189)	KAT	CAST	On Demand	Manually
SHA2-256 (A4190)	KAT	CAST	On Demand	Manually
SHA2-256 (A4192)	KAT	CAST	On Demand	Manually
SHA2-256 (A4193)	KAT	CAST	On Demand	Manually
SHA2-256 (A6709)	KAT	CAST	On Demand	Manually
SHA2-384 (A3860)	KAT	CAST	On Demand	Manually
SHA2-384 (A3861)	KAT	CAST	On Demand	Manually
SHA2-384 (A3862)	KAT	CAST	On Demand	Manually
SHA2-384 (A3885)	KAT	CAST	On Demand	Manually
SHA2-384 (A3886)	KAT	CAST	On Demand	Manually
SHA2-384 (A3887)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A3888)	KAT	CAST	On Demand	Manually
SHA2-384 (A3889)	KAT	CAST	On Demand	Manually
SHA2-384 (A3890)	KAT	CAST	On Demand	Manually
SHA2-384 (A3895)	KAT	CAST	On Demand	Manually
SHA2-384 (A4160)	KAT	CAST	On Demand	Manually
SHA2-384 (A4161)	KAT	CAST	On Demand	Manually
SHA2-384 (A4162)	KAT	CAST	On Demand	Manually
SHA2-384 (A4176)	KAT	CAST	On Demand	Manually
SHA2-384 (A4177)	KAT	CAST	On Demand	Manually
SHA2-384 (A4180)	KAT	CAST	On Demand	Manually
SHA2-384 (A4189)	KAT	CAST	On Demand	Manually
SHA2-384 (A4190)	KAT	CAST	On Demand	Manually
SHA2-384 (A4192)	KAT	CAST	On Demand	Manually
SHA2-384 (A4193)	KAT	CAST	On Demand	Manually
SHA2-384 (A6709)	KAT	CAST	On Demand	Manually
SHA2-512 (A3860)	KAT	CAST	On Demand	Manually
SHA2-512 (A3861)	KAT	CAST	On Demand	Manually
SHA2-512 (A3862)	KAT	CAST	On Demand	Manually
SHA2-512 (A3885)	KAT	CAST	On Demand	Manually
SHA2-512 (A3886)	KAT	CAST	On Demand	Manually
SHA2-512 (A3887)	KAT	CAST	On Demand	Manually
SHA2-512 (A3888)	KAT	CAST	On Demand	Manually
SHA2-512 (A3889)	KAT	CAST	On Demand	Manually
SHA2-512 (A3890)	KAT	CAST	On Demand	Manually
SHA2-512 (A3895)	KAT	CAST	On Demand	Manually
SHA2-512 (A4160)	KAT	CAST	On Demand	Manually
SHA2-512 (A4161)	KAT	CAST	On Demand	Manually
SHA2-512 (A4162)	KAT	CAST	On Demand	Manually
SHA2-512 (A4176)	KAT	CAST	On Demand	Manually
SHA2-512 (A4177)	KAT	CAST	On Demand	Manually
SHA2-512 (A4180)	KAT	CAST	On Demand	Manually
SHA2-512 (A4189)	KAT	CAST	On Demand	Manually
SHA2-512 (A4190)	KAT	CAST	On Demand	Manually
SHA2-512 (A4192)	KAT	CAST	On Demand	Manually
SHA2-512 (A4193)	KAT	CAST	On Demand	Manually
SHA2-512 (A6709)	KAT	CAST	On Demand	Manually
SHA3-224 (A3863)	KAT	CAST	On Demand	Manually
SHA3-224 (A4163)	KAT	CAST	On Demand	Manually
SHA3-256 (A3863)	KAT	CAST	On Demand	Manually
SHA3-256 (A4163)	KAT	CAST	On Demand	Manually
SHA3-384 (A3863)	KAT	CAST	On Demand	Manually
SHA3-384 (A4163)	KAT	CAST	On Demand	Manually
SHA3-512 (A3863)	KAT	CAST	On Demand	Manually
SHA3-512 (A4163)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4162)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4189)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4190)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4192)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3862)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3885)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3886)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A3887)	KAT	CAST	On Demand	Manually

Table 24: Conditional Periodic Information

10.4 Error States

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

Table 25: Error States

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

10.5 Operator Initiation of Self-Tests

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

11 Life-Cycle Assurance

11.1 Startup Procedures

The module is distributed as a part of the Oracle Linux 8 (OL8) and Oracle Linux 9 (OL9) RPM packages kernel-uek-5.15.0-303.171.5.2.2.el8uek and kernel-uek-5.15.0-303.171.5.2.2.el9uek, libkcapi-1.2.0-2.0.1.el8 and libkcapi-1.3.1-3.0.1.el9, libkcapi-hmaccalc-1.2.0-2.0.1.el8 and libkcapi-hmaccalc-1.3.1-3.0.1.el9.

The modules can achieve the approved mode by:

- For installation add the fips=1 option to the kernel command line during the system installation. During the software selection stage, do not install any third-party software.
- Switching the system into the approved mode after the installation. Execute the fips-mode-setup --enable command. Restart the system.

In both cases, the Crypto Officer must verify the OL8 and OL9 systems operate in the approved mode by executing the fips-mode-setup --check command, which should output “FIPS mode is enabled.”

After installation of the kernel-uek-5.15.0-303.171.5.2.2.el8uek and kernel-uek-5.15.0-303.171.5.2.2.el9uek, libkcapi-1.2.0-2.0.1.el8 and libkcapi-1.3.1-3.0.1.el9, libkcapi-hmaccalc-1.2.0-2.0.1.el8 and libkcapi-hmaccalc-1.3.1-3.0.1.el9 RPM packages, the Crypto Officer must execute the “cat /proc/sys/crypto/fips_name” command. The Crypto Officer must ensure that the proper name is listed in the output as follows:

Oracle Linux 8:

Oracle Linux 8 Unbreakable Enterprise Kernel 7 Crypto API

Oracle Linux 9:

Oracle Linux 9 Unbreakable Enterprise Kernel 7 Crypto API

Then, the Crypto Officer must execute the “cat /proc/sys/crypto/fips_version” and “rpm -q libkcapi” commands. These commands must output the following (one line per output):

Oracle Linux 8 Intel and AMD Platforms:

5.15.0-303.171.5.2.2.el8uek.x86_64

libkcapi-1.2.0-2.0.1.el8.x86_64

Oracle Linux 8 Ampere Platform:

5.15.0-303.171.5.2.2.el8uek.aarch64

libkcapi-1.2.0-2.0.1.el8.aarch64

Oracle Linux 9 Intel and AMD Platforms:

5.15.0-303.171.5.2.2.el9uek.x86_64
libkcapi-1.3.1-3.0.1.el9.x86_64

Oracle Linux 9 Ampere Platform:

5.15.0-303.171.5.2.2.el9uek.aarch64

libkcapi-1.3.1-3.0.1.el9.aarch64

Oracle Linux 9 Ampere Platform:

5.15.0-303.171.5.2.2.el9uek.aarch64

libkcapi-1.3.1-3.0.1.el9.aarch64

11.2 Administrator Guidance

The Approved and non-Approved modes of operation are specified in section 2.4. The administrative functions are specified in the Approved Services table. All the logical interfaces are specified in section 3.1. The requirements and restrictions that shall be considered when operating the module in approved mode are specified in section 2.7 and section 6. The installation, initialization, and startup procedures specified in section 11.1 shall be followed.

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.4 Maintenance Requirements

There are no maintenance requirements.

11.5 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 kernel-uek-5.15.0-303.171.5.2.2.el8uek and kernel-uek-5.15.0-303.171.5.2.2.el9uek, libkcapi-1.2.0-2.0.1.el8 and libkcapi-1.3.1-3.0.1.el9, libkcapi-hmaccalc-1.2.0-2.0.1.el8 and libkcapi-hmaccalc-1.3.1-3.0.1.el9 RPM packages can be uninstalled from the Oracle Linux 8 and Oracle Linux 9 systems.



12 Mitigation of Other Attacks

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

Appendix A Glossary and Abbreviations

AES	Advanced Encryption Standard
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
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliiptic Curve Digital Signature Algorithm
ENT (NP)	Non-physical Entropy Source
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HKDF	HMAC-based Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
IPsec	Internet Protocol Security
KAT	Known Answer Test
KBKDF	Key-based Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B References

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, April 2026 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	Secure Hash Standard (SHS) March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	Digital Signature Standard (DSS) July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 197	Advanced Encryption Standard November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) May 2003 https://www.ietf.org/rfc/rfc3526.txt
SP 800-38A	Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A Addendum	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode October 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices January 2010 https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-56Ar3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
SP 800-56Cr2	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 800-131Ar2	Transitioning the Use of Cryptographic Algorithms and Key Lengths March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.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