Amazon Web Services, Inc

AWS-LC 3.0 Cryptographic Module (static)

FIPS 140-3 Non-Proprietary Security Policy

Document version: 1.0

Last update: 2024-12-06

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version AWS-LC FIPS 3.0.0 of the AWS-LC 3.0 Cryptographic Module (static). 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.

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 AWS-LC 3.0 Cryptographic Module (static) 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 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.

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 AWS-LC 3.0 Cryptographic Module (static) (hereafter referred to as “the module”) provides cryptographic services to applications running in the user space of the underlying operating system through a C language Application Program Interface (API).

Module Type: Software

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The block diagram in Figure 1 shows the cryptographic boundary of the module, its interfaces with the operational environment and the flow of information between the module and operator (depicted through the arrows).

The cryptographic boundary is defined as the AWS-LC 3.0 Cryptographic Module (static) which is a cryptographic library consisting of the bcm.o file (version AWS-LC FIPS 3.0.0). This file is statically linked to the userspace application during the compilation process.

Tested Operational Environment’s Physical Perimeter (TOEPP):

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

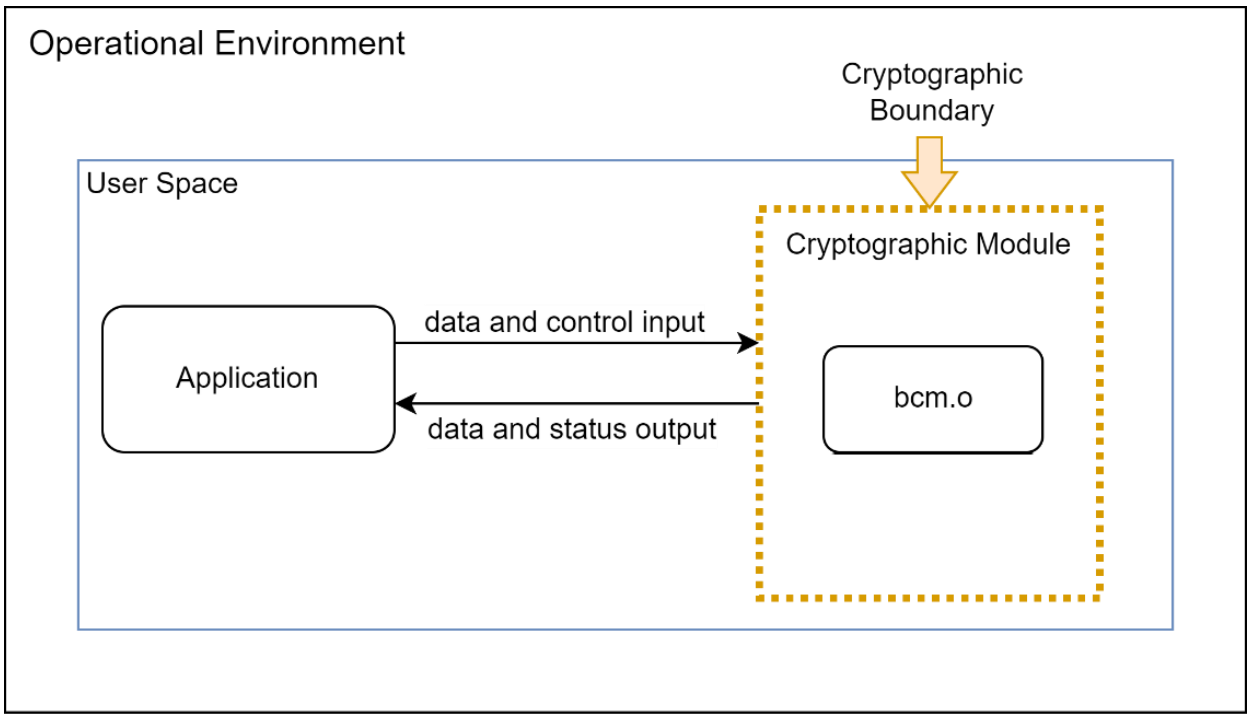

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
bcm.o on Amazon Linux 2023 on Graviton4 on r8g.metal-24xl	AWS-LC FIPS 3.0.0	N/A	HMAC-SHA2-256
bcm.o on Amazon Linux 2023 on Intel Xeon Platinum 8375C on c6i.metal	AWS-LC FIPS 3.0.0	N/A	HMAC-SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Amazon Linux 2023	r8g.metal-24xl	Graviton4	Yes	N/A	AWS-LC FIPS 3.0.0
Amazon Linux 2023	c6i.metal	Intel Xeon Platinum 8375C	Yes	N/A	AWS-LC FIPS 3.0.0
Amazon Linux 2023	r8g.metal-24xl	Graviton4	No	N/A	AWS-LC FIPS 3.0.0
Amazon Linux 2023	c6i.metal	Intel Xeon Platinum 8375C	No	N/A	AWS-LC FIPS 3.0.0

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

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

N/A for this module.

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

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered whenever an approved service is requested.	Approved	Equivalent to the indicator of the requested service 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 4.3

Table 4: Modes List and Description

Mode Change Instructions and Status:

When the module starts up successfully, after passing the pre-operational self-test and the cryptographic algorithms self-tests (CASTs), the module is operating in the approved mode of operation by default and can only be transitioned into the non-approved mode by calling one of the non-approved services listed in the *Non-Approved Services* table. The module will transition back to approved mode when approved service is called. Section 4.3 provides details on the service indicator implemented by the module. The service indicator identifies when an approved service is called.

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	A6283	-	SP 800-38A
AES-CBC	A6286	-	SP 800-38A
AES-CBC	A6292	-	SP 800-38A
AES-CBC	A6296	-	SP 800-38A
AES-CBC	A6301	-	SP 800-38A
AES-CBC	A6306	-	SP 800-38A
AES-CCM	A6283	-	SP 800-38C
AES-CCM	A6286	-	SP 800-38C
AES-CCM	A6292	-	SP 800-38C
AES-CCM	A6296	-	SP 800-38C
AES-CCM	A6301	-	SP 800-38C
AES-CCM	A6306	-	SP 800-38C
AES-CMAC	A6283	-	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A6286	-	SP 800-38B
AES-CMAC	A6292	-	SP 800-38B
AES-CMAC	A6296	-	SP 800-38B
AES-CMAC	A6301	-	SP 800-38B
AES-CMAC	A6306	-	SP 800-38B
AES-CTR	A6283	-	SP 800-38A
AES-CTR	A6286	-	SP 800-38A
AES-CTR	A6292	-	SP 800-38A
AES-CTR	A6296	-	SP 800-38A
AES-CTR	A6301	-	SP 800-38A
AES-CTR	A6306	-	SP 800-38A
AES-ECB	A6283	-	SP 800-38A
AES-ECB	A6284	-	SP 800-38A
AES-ECB	A6285	-	SP 800-38A
AES-ECB	A6286	-	SP 800-38A
AES-ECB	A6287	-	SP 800-38A
AES-ECB	A6292	-	SP 800-38A
AES-ECB	A6293	-	SP 800-38A
AES-ECB	A6296	-	SP 800-38A
AES-ECB	A6297	-	SP 800-38A
AES-ECB	A6298	-	SP 800-38A
AES-ECB	A6299	-	SP 800-38A
AES-ECB	A6300	-	SP 800-38A
AES-ECB	A6301	-	SP 800-38A
AES-ECB	A6302	-	SP 800-38A
AES-ECB	A6303	-	SP 800-38A
AES-ECB	A6304	-	SP 800-38A
AES-ECB	A6305	-	SP 800-38A
AES-ECB	A6306	-	SP 800-38A
AES-ECB	A6307	-	SP 800-38A
AES-ECB	A6308	-	SP 800-38A
AES-ECB	A6309	-	SP 800-38A
AES-ECB	A6310	-	SP 800-38A
AES-GCM	A6284	-	SP 800-38D
AES-GCM	A6285	-	SP 800-38D
AES-GCM	A6287	-	SP 800-38D
AES-GCM	A6293	-	SP 800-38D
AES-GCM	A6297	-	SP 800-38D
AES-GCM	A6298	-	SP 800-38D
AES-GCM	A6299	-	SP 800-38D
AES-GCM	A6300	-	SP 800-38D
AES-GCM	A6302	-	SP 800-38D
AES-GCM	A6303	-	SP 800-38D
AES-GCM	A6304	-	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A6305	-	SP 800-38D
AES-GCM	A6307	-	SP 800-38D
AES-GCM	A6308	-	SP 800-38D
AES-GCM	A6309	-	SP 800-38D
AES-GCM	A6310	-	SP 800-38D
AES-GMAC	A6284	-	SP 800-38D
AES-GMAC	A6285	-	SP 800-38D
AES-GMAC	A6287	-	SP 800-38D
AES-GMAC	A6293	-	SP 800-38D
AES-GMAC	A6297	-	SP 800-38D
AES-GMAC	A6298	-	SP 800-38D
AES-GMAC	A6299	-	SP 800-38D
AES-GMAC	A6300	-	SP 800-38D
AES-GMAC	A6302	-	SP 800-38D
AES-GMAC	A6303	-	SP 800-38D
AES-GMAC	A6304	-	SP 800-38D
AES-GMAC	A6305	-	SP 800-38D
AES-GMAC	A6307	-	SP 800-38D
AES-GMAC	A6308	-	SP 800-38D
AES-GMAC	A6309	-	SP 800-38D
AES-GMAC	A6310	-	SP 800-38D
AES-KW	A6283	-	SP 800-38F
AES-KW	A6286	-	SP 800-38F
AES-KW	A6292	-	SP 800-38F
AES-KW	A6296	-	SP 800-38F
AES-KW	A6301	-	SP 800-38F
AES-KW	A6306	-	SP 800-38F
AES-KWP	A6283	-	SP 800-38F
AES-KWP	A6286	-	SP 800-38F
AES-KWP	A6292	-	SP 800-38F
AES-KWP	A6296	-	SP 800-38F
AES-KWP	A6301	-	SP 800-38F
AES-KWP	A6306	-	SP 800-38F
AES-XTS Testing Revision 2.0	A6283	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6286	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6292	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6296	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6301	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6306	-	SP 800-38E
AES-XTS Testing Revision 2.0	A6311	-	SP 800-38E
Counter DRBG	A6283	-	SP 800-90A Rev. 1
Counter DRBG	A6286	-	SP 800-90A Rev. 1
Counter DRBG	A6292	-	SP 800-90A Rev. 1
Counter DRBG	A6296	-	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A6301	-	SP 800-90A Rev. 1
Counter DRBG	A6306	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6288	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6289	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6291	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6295	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6312	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6313	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6314	-	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6315	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6288	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6289	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6291	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6295	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6312	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6313	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6314	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6315	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6288	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6289	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6291	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6295	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6312	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6313	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6314	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6315	-	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A6288	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6289	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6291	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6295	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6312	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6313	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6314	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A6315	-	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A6288	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6289	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6291	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6295	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6312	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6313	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6314	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6315	-	FIPS 186-5
EDDSA KeyGen	A6288	-	FIPS 186-5
EDDSA KeyGen	A6289	-	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
EDDSA KeyGen	A6291	-	FIPS 186-5
EDDSA KeyGen	A6295	-	FIPS 186-5
EDDSA KeyGen	A6312	-	FIPS 186-5
EDDSA KeyGen	A6313	-	FIPS 186-5
EDDSA KeyGen	A6314	-	FIPS 186-5
EDDSA KeyGen	A6315	-	FIPS 186-5
EDDSA SigGen	A6288	-	FIPS 186-5
EDDSA SigGen	A6289	-	FIPS 186-5
EDDSA SigGen	A6291	-	FIPS 186-5
EDDSA SigGen	A6295	-	FIPS 186-5
EDDSA SigGen	A6312	-	FIPS 186-5
EDDSA SigGen	A6313	-	FIPS 186-5
EDDSA SigGen	A6314	-	FIPS 186-5
EDDSA SigGen	A6315	-	FIPS 186-5
EDDSA SigVer	A6288	-	FIPS 186-5
EDDSA SigVer	A6289	-	FIPS 186-5
EDDSA SigVer	A6291	-	FIPS 186-5
EDDSA SigVer	A6295	-	FIPS 186-5
EDDSA SigVer	A6312	-	FIPS 186-5
EDDSA SigVer	A6313	-	FIPS 186-5
EDDSA SigVer	A6314	-	FIPS 186-5
EDDSA SigVer	A6315	-	FIPS 186-5
HMAC-SHA-1	A6288	-	FIPS 198-1
HMAC-SHA-1	A6289	-	FIPS 198-1
HMAC-SHA-1	A6291	-	FIPS 198-1
HMAC-SHA-1	A6295	-	FIPS 198-1
HMAC-SHA-1	A6312	-	FIPS 198-1
HMAC-SHA-1	A6313	-	FIPS 198-1
HMAC-SHA-1	A6314	-	FIPS 198-1
HMAC-SHA-1	A6315	-	FIPS 198-1
HMAC-SHA2-224	A6288	-	FIPS 198-1
HMAC-SHA2-224	A6289	-	FIPS 198-1
HMAC-SHA2-224	A6291	-	FIPS 198-1
HMAC-SHA2-224	A6295	-	FIPS 198-1
HMAC-SHA2-224	A6312	-	FIPS 198-1
HMAC-SHA2-224	A6313	-	FIPS 198-1
HMAC-SHA2-224	A6314	-	FIPS 198-1
HMAC-SHA2-224	A6315	-	FIPS 198-1
HMAC-SHA2-256	A6288	-	FIPS 198-1
HMAC-SHA2-256	A6289	-	FIPS 198-1
HMAC-SHA2-256	A6291	-	FIPS 198-1
HMAC-SHA2-256	A6295	-	FIPS 198-1
HMAC-SHA2-256	A6312	-	FIPS 198-1
HMAC-SHA2-256	A6313	-	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A6314	-	FIPS 198-1
HMAC-SHA2-256	A6315	-	FIPS 198-1
HMAC-SHA2-384	A6288	-	FIPS 198-1
HMAC-SHA2-384	A6289	-	FIPS 198-1
HMAC-SHA2-384	A6291	-	FIPS 198-1
HMAC-SHA2-384	A6295	-	FIPS 198-1
HMAC-SHA2-384	A6312	-	FIPS 198-1
HMAC-SHA2-384	A6313	-	FIPS 198-1
HMAC-SHA2-384	A6314	-	FIPS 198-1
HMAC-SHA2-384	A6315	-	FIPS 198-1
HMAC-SHA2-512	A6288	-	FIPS 198-1
HMAC-SHA2-512	A6289	-	FIPS 198-1
HMAC-SHA2-512	A6291	-	FIPS 198-1
HMAC-SHA2-512	A6295	-	FIPS 198-1
HMAC-SHA2-512	A6312	-	FIPS 198-1
HMAC-SHA2-512	A6313	-	FIPS 198-1
HMAC-SHA2-512	A6314	-	FIPS 198-1
HMAC-SHA2-512	A6315	-	FIPS 198-1
HMAC-SHA2-512/224	A6288	-	FIPS 198-1
HMAC-SHA2-512/224	A6289	-	FIPS 198-1
HMAC-SHA2-512/224	A6291	-	FIPS 198-1
HMAC-SHA2-512/224	A6295	-	FIPS 198-1
HMAC-SHA2-512/224	A6312	-	FIPS 198-1
HMAC-SHA2-512/224	A6313	-	FIPS 198-1
HMAC-SHA2-512/224	A6314	-	FIPS 198-1
HMAC-SHA2-512/224	A6315	-	FIPS 198-1
HMAC-SHA2-512/256	A6288	-	FIPS 198-1
HMAC-SHA2-512/256	A6289	-	FIPS 198-1
HMAC-SHA2-512/256	A6291	-	FIPS 198-1
HMAC-SHA2-512/256	A6295	-	FIPS 198-1
HMAC-SHA2-512/256	A6312	-	FIPS 198-1
HMAC-SHA2-512/256	A6313	-	FIPS 198-1
HMAC-SHA2-512/256	A6314	-	FIPS 198-1
HMAC-SHA2-512/256	A6315	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6288	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6289	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6291	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6295	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6312	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6313	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6314	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6315	-	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A6288	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6289	-	SP 800-56C Rev. 2

Algorithm	CAVP Cert	Properties	Reference
KDA HKDF Sp800-56Cr1	A6291	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6295	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6312	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6313	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6314	-	SP 800-56C Rev. 2
KDA HKDF Sp800-56Cr1	A6315	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6288	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6289	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6291	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6295	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6312	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6313	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6314	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A6315	-	SP 800-56C Rev. 2
KDF SP800-108	A6288	-	SP 800-108 Rev. 1
KDF SP800-108	A6289	-	SP 800-108 Rev. 1
KDF SP800-108	A6291	-	SP 800-108 Rev. 1
KDF SP800-108	A6295	-	SP 800-108 Rev. 1
KDF SP800-108	A6312	-	SP 800-108 Rev. 1
KDF SP800-108	A6313	-	SP 800-108 Rev. 1
KDF SP800-108	A6314	-	SP 800-108 Rev. 1
KDF SP800-108	A6315	-	SP 800-108 Rev. 1
KDF SSH (CVL)	A6288	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6289	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6291	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6295	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6312	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6313	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6314	-	SP 800-135 Rev. 1
KDF SSH (CVL)	A6315	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6288	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6289	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6291	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6295	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6312	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6313	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6314	-	SP 800-135 Rev. 1
KDF TLS (CVL)	A6315	-	SP 800-135 Rev. 1
ML-KEM EncapDecap	A6288	-	
ML-KEM EncapDecap	A6289	-	
ML-KEM EncapDecap	A6291	-	
ML-KEM EncapDecap	A6295	-	
ML-KEM EncapDecap	A6312	-	
ML-KEM EncapDecap	A6313	-	

Algorithm	CAVP Cert	Properties	Reference
ML-KEM EncapDecap	A6314	-	
ML-KEM EncapDecap	A6315	-	
ML-KEM KeyGen	A6288	-	
ML-KEM KeyGen	A6289	-	
ML-KEM KeyGen	A6291	-	
ML-KEM KeyGen	A6295	-	
ML-KEM KeyGen	A6312	-	
ML-KEM KeyGen	A6313	-	
ML-KEM KeyGen	A6314	-	
ML-KEM KeyGen	A6315	-	
PBKDF	A6288	-	SP 800-132
PBKDF	A6289	-	SP 800-132
PBKDF	A6291	-	SP 800-132
PBKDF	A6295	-	SP 800-132
PBKDF	A6312	-	SP 800-132
PBKDF	A6313	-	SP 800-132
PBKDF	A6314	-	SP 800-132
PBKDF	A6315	-	SP 800-132
RSA KeyGen (FIPS186-5)	A6288	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6289	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6290	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6291	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6295	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6312	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6313	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6314	-	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6315	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6288	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6289	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6290	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6291	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6295	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6312	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6313	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6314	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A6315	-	FIPS 186-5
RSA SigVer (FIPS186-4)	A6288	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6289	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6290	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6291	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6295	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6312	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6313	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A6314	-	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-4)	A6315	-	FIPS 186-4
RSA SigVer (FIPS186-5)	A6288	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6289	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6290	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6291	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6295	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6312	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6313	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6314	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A6315	-	FIPS 186-5
SHA-1	A6288	-	FIPS 180-4
SHA-1	A6289	-	FIPS 180-4
SHA-1	A6291	-	FIPS 180-4
SHA-1	A6295	-	FIPS 180-4
SHA-1	A6312	-	FIPS 180-4
SHA-1	A6313	-	FIPS 180-4
SHA-1	A6314	-	FIPS 180-4
SHA-1	A6315	-	FIPS 180-4
SHA2-224	A6288	-	FIPS 180-4
SHA2-224	A6289	-	FIPS 180-4
SHA2-224	A6291	-	FIPS 180-4
SHA2-224	A6295	-	FIPS 180-4
SHA2-224	A6312	-	FIPS 180-4
SHA2-224	A6313	-	FIPS 180-4
SHA2-224	A6314	-	FIPS 180-4
SHA2-224	A6315	-	FIPS 180-4
SHA2-256	A6288	-	FIPS 180-4
SHA2-256	A6289	-	FIPS 180-4
SHA2-256	A6291	-	FIPS 180-4
SHA2-256	A6295	-	FIPS 180-4
SHA2-256	A6312	-	FIPS 180-4
SHA2-256	A6313	-	FIPS 180-4
SHA2-256	A6314	-	FIPS 180-4
SHA2-256	A6315	-	FIPS 180-4
SHA2-384	A6288	-	FIPS 180-4
SHA2-384	A6289	-	FIPS 180-4
SHA2-384	A6291	-	FIPS 180-4
SHA2-384	A6295	-	FIPS 180-4
SHA2-384	A6312	-	FIPS 180-4
SHA2-384	A6313	-	FIPS 180-4
SHA2-384	A6314	-	FIPS 180-4
SHA2-384	A6315	-	FIPS 180-4
SHA2-512	A6288	-	FIPS 180-4
SHA2-512	A6289	-	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512	A6291	-	FIPS 180-4
SHA2-512	A6295	-	FIPS 180-4
SHA2-512	A6312	-	FIPS 180-4
SHA2-512	A6313	-	FIPS 180-4
SHA2-512	A6314	-	FIPS 180-4
SHA2-512	A6315	-	FIPS 180-4
SHA2-512/224	A6288	-	FIPS 180-4
SHA2-512/224	A6289	-	FIPS 180-4
SHA2-512/224	A6291	-	FIPS 180-4
SHA2-512/224	A6295	-	FIPS 180-4
SHA2-512/224	A6312	-	FIPS 180-4
SHA2-512/224	A6313	-	FIPS 180-4
SHA2-512/224	A6314	-	FIPS 180-4
SHA2-512/224	A6315	-	FIPS 180-4
SHA2-512/256	A6288	-	FIPS 180-4
SHA2-512/256	A6289	-	FIPS 180-4
SHA2-512/256	A6291	-	FIPS 180-4
SHA2-512/256	A6295	-	FIPS 180-4
SHA2-512/256	A6312	-	FIPS 180-4
SHA2-512/256	A6313	-	FIPS 180-4
SHA2-512/256	A6314	-	FIPS 180-4
SHA2-512/256	A6315	-	FIPS 180-4
SHA3-224	A6294	-	FIPS 202
SHA3-256	A6294	-	FIPS 202
SHA3-384	A6294	-	FIPS 202
SHA3-512	A6294	-	FIPS 202
SHAKE-128	A6294	-	FIPS 202
SHAKE-256	A6294	-	FIPS 202

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

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

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

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

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
MD5	Allowed per IG 2.4.A	Message Digest used in TLS 1.0/1.1 KDF only

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES with OFB or CFB1, CFB8, CFB128 modes	Encryption, Decryption
AES GCM, GCM, GMAC, XTS with keys not listed in Table 5	Encryption, Decryption
AES using aes_*_generic function	Encryption, Decryption
RSA encryption primitive with PKCS#1 v1.5 and OAEP padding	Encryption
AES GMAC using aes_*_generic	Message Authentication Generation
Curve secp256k1	Signature Generation, Signature Verification, Shared Secret Computation
Diffie Hellman	Shared Secret Computation
HMAC-MD4, HMAC-MD5, HMAC-SHA-3, HMAC-RIPEMD-160	Message Authentication Generation
MD4	Message Digest
MD5 (outside of TLS)	Message Digest
RIPEMD-160	Message Digest
RSA using RSA_generate_key_ex	Key Generation
ECDSA using EC_KEY_generate_key	Key Generation
RSA using keys less than 2048 bits	Signature Generation
SHA-1	Signature Generation
RSA using keys less than 1024 bits	Signature Verification
RSA without hashing	Sign/Verify primitive operations
TLS KDF using any SHA algorithms other than SHA2-256, SHA2-384, SHA2-512; or TLS KDF using non-extended master secret	Key Derivation
RSA	Key Encapsulation/Un-encapsulation

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Shared Secret Computation with EC Diffie-Hellman	KAS-SSC	SP800-56Arev3. KAS-ECC-SSC per IG D.F Scenario 2 path (1)	Curves:P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of strength	KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3

Name	Type	Description	Properties	Algorithms
				KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3 KAS-ECC-SSC Sp800-56Ar3
Key Wrapping/Unwrapping with AES KW, AES-KWP	KTS-Wrap	SP800-38F. KTS (key wrapping, key unwrapping) per IG D.G	AES keys:128, 192, 256 bits with 128-256 bits of strength	AES-KW AES-KWP AES-KW AES-KWP AES-KW AES-KWP AES-KW AES-KWP AES-KW AES-KWP AES-KW AES-KWP
Key Wrapping/Unwrapping with AES GCM	KTS-Wrap	SP800-38D. KTS (key wrapping, key unwrapping) per IG D.G.	AES keys:128 and 256 bits with 128 and 256 bits of strength	AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM
Key Wrapping/Unwrapping with AES CCM	KTS-Wrap	SP800-38C. KTS (key wrapping, key unwrapping) per IG D.G	AES keys:128 bits with 128 bits of strength	AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM
Encryption/Decryption with AES	BC-UnAuth	SP800-38A and SP 800-38E. Encryption and Decryption	AES keys:128, 192, 256 bits keys with 128-256 bits of strength	AES-CBC AES-CTR AES-ECB AES-XTS Testing Revision 2.0 AES-ECB AES-ECB AES-CBC AES-CTR AES-ECB AES-CTR AES-XTS Testing Revision 2.0 AES-ECB AES-CBC

Name	Type	Description	Properties	Algorithms
				AES-CTR AES-ECB AES-XTS Testing Revision 2.0 AES-ECB AES-CBC AES-CTR AES-ECB AES-XTS Testing Revision 2.0 AES-ECB AES-ECB AES-ECB AES-ECB AES-CBC AES-CTR AES-ECB AES-XTS Testing Revision 2.0 AES-ECB AES-ECB AES-ECB AES-ECB AES-CBC AES-CTR AES-ECB AES-XTS Testing Revision 2.0 AES-ECB AES-ECB AES-ECB AES-ECB AES-XTS Testing Revision 2.0
Signature Generation with RSA	DigSig-SigGen	FIPS186-5. Digital signature generation. Per IG C.F, RSA SigGen was CAVP tested with moduli sizes 2048, 3072, 4096 bits. The module supports moduli sizes larger than 4096 bits.	RSA keys:2048, 3072, 4096 bits with 112-150 bits of strength	RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) RSA SigGen (FIPS186-5) SHA2-224

Name	Type	Description	Properties	Algorithms
				SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Signature Generation with ECDSA	DigSig-SigGen	FIPS186-5. Digital signature generation	Curves:P-224, P-256, P-384, P-521 with 112-256 bits of strength	ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen

Name	Type	Description	Properties	Algorithms
				(FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) ECDSA SigGen (FIPS186-5) SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA3-224 SHA3-256

Name	Type	Description	Properties	Algorithms
				SHA3-384 SHA3-512
Signature Generation with EDDSA	DigSig-SigGen	FIPS186-5. Digital signature generation	Curve: ED-25519 with 128 bits of strength	EDDSA SigGen EDDSA SigGen EDDSA SigGen EDDSA SigGen EDDSA SigGen EDDSA SigGen EDDSA SigGen EDDSA SigGen
Key Generation with RSA	AsymKeyPair-KeyGen	FIPS186-5. Key generation. Per IG C.F, RSA KeyGen was CAVP tested with moduli sizes of 2048, 3072, 4096, 6144, 8192 bits. The number of Miller-Rabin tests is compliant with Table B.1 of FIPS 186-5.	RSA keys:2048, 3072, 4096, 6144, 8192 bits with 112, 128, 150, 178, 200 bits of key strength	RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5) RSA KeyGen (FIPS186-5)
Key Generation with ECDSA	AsymKeyPair-KeyGen	FIPS186-5. Key generation	Curves:P-224, P-256, P-384, P-521 with 112-256 bits of strength	ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5) ECDSA KeyGen (FIPS186-5)
Key Generation with EDDSA	AsymKeyPair-KeyGen	FIPS186-5. Key generation	Curve:ED-25519 with 128 bits of strength	EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen EDDSA KeyGen

Name	Type	Description	Properties	Algorithms
Key Generation with ML-KEM	AsymKeyPair-KeyGen	FIPS203, Section 7.1. Key generation	ML-KEM keys: ML-KEM-512 (800, 1632) bytes; ML-KEM-768 (1184, 2400) bytes; ML-KEM-1024 (1568, 3168) bytes with 128-256 bits of strength	ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen ML-KEM KeyGen
Signature Verification with ECDSA	DigSig-SigVer	FIPS186-5. Digital signature verification	Curves:P-224, P-256, P-384, P-521 with 112-256 bits of strength	ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-5) SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256

Name	Type	Description	Properties	Algorithms
				SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512 ECDSA SigVer (FIPS186-4) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5) ECDSA SigVer (FIPS186-5)
Signature Verification with EDDSA	DigSig-SigVer	FIPS186-5. Digital signature verification	Curve:ED-25519 with 128 bits of strength	EDDSA SigVer EDDSA SigVer EDDSA SigVer EDDSA SigVer EDDSA SigVer EDDSA SigVer

Name	Type	Description	Properties	Algorithms
				EDDSA SigVer EDDSA SigVer
Signature Verification with RSA	DigSig-SigVer	FIPS186-4 (Legacy) and FIPS186-5. Digital signature verification. Per IG C.F, RSA SigVer was CAVP tested with moduli sizes 1024, 2048, 3072, 4096 bits. The module supports moduli sizes larger than 4096 bits.	RSA keys:1024, 2048, 3072, 4096 bits with 80-150 bits of strength	RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) RSA SigVer (FIPS186-5) SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256

Name	Type	Description	Properties	Algorithms
				SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Key Verification with ECDSA	AsymKeyPair-KeyVer	FIPS186-5. Key verification	Curves:P-224, P-256, P-384, P-521 with 112-256 bits of strength	ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5) ECDSA KeyVer (FIPS186-5)
Encapsulation/Decapsulation with ML-KEM	KTS-Encap	FIPS203, Section 7.2 and 7.3.	ML-KEM keys:ML-KEM-512 (800,	ML-KEM EncapDecap

Name	Type	Description	Properties	Algorithms
		Encapsulation and decapsulation	1632) bytes; ML-KEM-768 (1184, 2400) bytes; ML-KEM-1024 (1568, 3168) bytes; with 128-256 bits of strength	ML-KEM EncapDecap ML-KEM EncapDecap ML-KEM EncapDecap ML-KEM EncapDecap ML-KEM EncapDecap ML-KEM EncapDecap ML-KEM EncapDecap
Key Derivation with TLS KDF	KAS-135KDF	SP800-135rev1. Key derivation	TLS KDF derived keys:112 to 256 bits with 112-256 bits of strength	KDF TLS KDF TLS KDF TLS KDF TLS KDF TLS KDF TLS KDF TLS KDF TLS
Key Derivation with SSH KDF	KAS-135KDF	SP800-135rev1. Key derivation	SSH KDF derived keys:128 to 512 bits with 112-256 bits of strength	KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH KDF SSH
Key Derivation with KDA HKDF	KAS-56CKDF	SP800-56Crev1. Key derivation	Shared secret:224-2048 bits with 112-256 bits of strength KDA HKDF derived keys:2048 bits with 112-256 bits of strength	KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1 KDA HKDF Sp800-56Cr1
Key Derivation with KDA OneStep	KAS-56CKDF	SP800-56Crev1. Key derivation	Shared secret:224-2048 bits with 112-256 bits of strength KDA OneStep derived keys:2048 bits with 112-256 bits of strength	KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep

Name	Type	Description	Properties	Algorithms
				SP800-56Cr2 KDA OneStep SP800-56Cr2 KDA OneStep SP800-56Cr2
Key Derivation with PBKDF	PBKDF	SP800-132. Key derivation	PBKDF derived keys:128 to 4096 bits with 112-256 bits of strength	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF
Key Derivation with KBKDF	KBKDF	SP800-108. Key based key derivation	KBKDF derived keys:2048 bits with 112-256 bits of strength Modes:Counter; Feedback	KDF SP800-108 KDF SP800-108 KDF SP800-108 KDF SP800-108 KDF SP800-108 KDF SP800-108 KDF SP800-108 KDF SP800-108
Message Digest with SHA	SHA	FIPS180-4 and FIPS202. Message digest using SHA	N/A: N/A	SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224

Name	Type	Description	Properties	Algorithms
				SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA2-512/224 SHA2-512/256 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Message Digest with SHAKE	XOF	FIPS202. Message digest using SHAKE	N/A: N/A	SHAKE-128 SHAKE-256
Random Number Generation with DRBG	DRBG	SP800-90ARev1. Random number generation	AES key:256 bits with 256 bits of strength; no derivation function; no prediction resistance	Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG Counter DRBG
Message Authentication Generation with HMAC	MAC	FIPS198-1. Message authentication generation	HMAC keys:112 to 524288 bits with 112-256 bits of strength SHA algorithm:SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-224 HMAC-SHA2-256

Name	Type	Description	Properties	Algorithms
				HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-512/224 HMAC-SHA2-

Name	Type	Description	Properties	Algorithms
				512/224 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512/256 HMAC-SHA2-512
Message Authentication Generation with AES	MAC	SP800-38B and SP800-38D Message authentication generation	AES keys:128 or 256 bits with 128 or 256 bits of strength	AES-CMAC AES-CMAC AES-CMAC AES-CMAC AES-CMAC AES-CMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC AES-GMAC
Authenticated Encryption/Decryption with AES CCM	BC-Auth	SP800-38C. Authenticated encryption and decryption	AES keys:128 bits with 128 bits of strength	AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM AES-CCM
Authenticated Encryption/Decryption with AES GCM	BC-Auth	SP800-38D. Authenticated encryption and decryption	AES keys:128 or 256 bits with 128 or 256 bits of strength Authenticated Encryption:Internal IV Modes 8.2.1 and 8.2.2 Authenticated Decryption:External IV	AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM

Name	Type	Description	Properties	Algorithms
				AES-GCM AES-GCM AES-GCM AES-GCM AES-GCM

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

GCM IV

The module offers three AES GCM implementations. The GCM IV generation for these implementations complies respectively with IG C.H under Scenario 1, Scenario 2, and Scenario 5. The GCM shall only be used in the context of the AES-GCM encryption executing under each scenario, and using the referenced APIs explained next.

Scenario 1, TLS 1.2

For TLS 1.2, the module offers the GCM implementation and uses the context of Scenario 1 of IG C.H. The module is compliant with SP800-52rev2 and the mechanism for IV generation is compliant with RFC5288. The module supports acceptable AES-GCM ciphersuites from Section 3.3.1 of SP800-52rev2.

The module explicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values of 2^{64-1} for a given session key. If this exhaustion condition is observed, the module returns an error indication to the calling application, which will then need to either abort the connection, or trigger a handshake to establish a new encryption 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.

Scenario 2, Random IV

In this implementation, the module offers interfaces for compliance with Scenario 2 of IG C.H and SP800-38D Section 8.2.2. The AES-GCM IV is generated randomly internal to the module using module’s approved DRBG. The DRBG seeds itself from the entropy source. The GCM IV is 96 bits in length. Per Section 9, this 96-bit IV contains 96 bits of entropy.

Scenario 5, TLS 1.3

August 2018, using the ciphersuites that explicitly select AES-GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The module supports acceptable AES-GCM ciphersuites from Section 3.3.1 of SP800-52rev2.

The module implements, within its boundary, an IV generation unit for TLS 1.3 that keeps control of the 64-bit counter value within the AES-GCM IV. If the exhaustion condition is observed, the module will return an error indication to the calling application, who will then need to either trigger a re-key of the session (i.e., a new key for AES-GCM), or terminate the connection.

In the event the module’s power is lost and restored, the consuming application must ensure that new AES-GCM keys encryption or decryption under this scenario are established. TLS

1.3 provides session resumption, but the resumption procedure derives new AES-GCM encryption keys.

AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E. The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit.

Key Derivation using SP 800-132 PBKDF2

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

- Derived keys shall only be used in storage applications. The MK shall not be used for other purposes. The module accepts a minimum length of 112 bits for the MK or DPK.
- Passwords or passphrases, used as an input for the PBKDF2, shall not be used as cryptographic Keys.
- The minimum length of the password or passphrase accepted by the module is 14 characters. This results in the estimated probability of guessing the password to be at most 10^{-14}. Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.
- A portion of the salt, with a length of at least 128 bits (this is verified by the module to determine the service is approved), shall be generated randomly using the SP 800-90Ar1 DRBG provided by the module.
- The iteration count shall be selected as large as possible, if the time required to generate the key using the entered password is acceptable for the users. The module restricts the minimum iteration count to be 1000.

Compliance to SP 800-56ARev3 assurances

The module offers ECDH shared secret computation services compliant to the SP 800-56ARev3 and meeting IG D.F scenario 2 path (1). To meet the required assurances listed in section 5.6 of SP 800-56ARev3, the module shall be used together with an application that implements the “TLS protocol” and the following steps shall be performed.

- The entity using the module, must use the module's "Key Pair Generation" service for generating ECDH ephemeral keys. This meets the assurances required by key pair owner defined in the section 5.6.2.1 of SP 800-56ARev3.
- As part of the module's shared secret computation (SSC) service, the module internally performs the public key validation on the peer's public key passed in as input to the SSC function. This meets the public key validity assurance required by the sections 5.6.2.2.1/5.6.2.2.2 of SP 800-56Arev3.
- The module does not support static keys therefore the "assurance of peer's possession of private key" is not applicable.

Legacy Algorithms

According to IG C.M, digital signature verification using RSA with a 1024-bits modulus is approved for legacy usage only. Digital signature verification using SHA-1 is approved for legacy usage only. The CAVP certificates for these algorithms are listed in the *Approved Algorithms* table. These legacy algorithms can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

The module provides an SP800-90Arev1-compliant Deterministic Random Bit Generator (DRBG) using CTR_DRBG mechanism with AES-256 for generation of key components of asymmetric keys, and random number generation. The DRBG is seeded with 256-bit of entropy input provided from an external entity to the module. This corresponds to scenario 2 (b) of IG 9.3.A i.e., the DRBG that receives a LOAD command with entropy obtained from inside the physical perimeter of the operational environment but outside of module's cryptographic boundary. The calling application shall use an entropy source that meets the security strength required for the CTR_DRBG as shown in NIST SP 800-90Arev1, Table 3 and should return an error if minimum strength cannot be met.

Per the IG 9.3.A requirement, the module includes the caveat "No assurance of the minimum strength of generated keys".

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800-133Rev2. When random values are required, they are obtained from the SP 800-90ARev1 approved DRBG, compliant with Section 4 of SP 800-133Rev2. The following methods are implemented:

- ECDSA KeyGen (FIPS 186-5, A.2.2 Rejection Sampling): P-224, P-256, P 384, P-521 elliptic curves with 112-256 bits of strength.
- EDDSA KeyGen (FIPS 186-5, A.2.3): ED-25519 with 128 bits of strength.
- RSA KeyGen (FIPS 186-5, A.1.3 Random Probable Primes): 2048, 3072, 4096, 6144, 8192 bits with 112, 128, 150, 178, 200 bits of key strength.
- ML-KEM KeyGen (FIPS 203, 5.1): (800, 1632 bytes), (1184, 2400 bytes), (1568, 3168 bytes) with 128, 192, 256 bits of key strength.

Additionally, the module implements the following key derivation methods per SP800-133Rev2 section 6.2:

- KDA HKDF (SP 800-56CRev1): 2048 bits with 112-256 bits of key strength
- KDA OneStep (SP 800-56CRev2): 2048 bits with 112-256 bits of key strength
- KBKDF (SP 800-108): 2048 bits with 112-256 bits of key strength
- PBKDF (SP 800-133Rev2, option 1a): 128-4096 bits with 112-256 bits of key strength
- SSH KDF (SP 800-135Rev1): 112-512 bits with 112-256 bits of key strength
- KDF TLS (SP 800-135Rev1): 112-256 bits with 112-256 bits of key strength

2.10 Key Establishment

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

2.11 Industry Protocols

The module implements the SSH key derivation function for use in the SSH protocol (RFC 4253 and RFC 6668).

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

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 10: Ports and Interfaces

As a Software module, the module interfaces are defined as Software or Firmware Module Interfaces (SMFI), and there are no physical ports. The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 11: Roles

The module does not support concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Encryption	Encryption	1	AES key, plaintext	Ciphertext	Encryption/Decryption with AES	Crypto Officer - AES Key: W,E
Decryption	Decryption	1	AES key, ciphertext	Plaintext	Encryption/Decryption with AES	Crypto Officer - AES Key: W,E
Authenticated Encryption	Authenticated Encryption	1	AES key, plaintext, IV	Ciphertext, MAC tag	Authenticated Encryption/Decryption with AES CCM Authenticated Encryption/Decryption with AES GCM	Crypto Officer - AES Key: W,E
Authenticated Decryption	Authenticated Decryption	1	AES key, ciphertext, IV, MAC tag	Plaintext or fail	Authenticated Encryption/Decryption with AES CCM Authenticated Encryption/Decryption with AES GCM	Crypto Officer - AES Key: W,E
Key Wrapping	Encrypting a key	1	AES key wrapping key, Key to be wrapped	Wrapped key	Key Wrapping/Unwrapping with AES KW, AES-KWP Key Wrapping/Unwrapping with AES GCM Key Wrapping/Unwrapping with AES CCM	Crypto Officer - AES Key: W,E
Key Unwrapping	Decrypting a key	1	AES key unwrapping key,	Unwrapped key or fail	Key Wrapping/Unwrapping with AES KW, AES-KWP	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			Key to be unwrapped		Key Wrapping/Unwrapping with AES GCM Key Wrapping/Unwrapping with AES CCM	- AES Key: W,E
Message Authentication Generation	MAC computation	1	AES key or HMAC key, message	MAC tag	Message Authentication Generation with HMAC Message Authentication Generation with AES	Crypto Officer - HMAC Key: W,E - AES Key: W,E
Message Digest	Generating message digest	1	Message	Message digest	Message Digest with SHA Message Digest with SHAKE	Crypto Officer
Random Number Generation	Generating random numbers	1	Output length	Random bytes	Random Number Generation with DRBG	Crypto Officer - Entropy Input: W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E
Key Generation	Generating a key pair	1	Modulus size / Curve	RSA public key, RSA private key / EC public key, EC private key, ML-KEM public key, ML-KEM private key	Key Generation with RSA Key Generation with ECDSA Key Generation with EDDSA Key Generation with ML-KEM	Crypto Officer - RSA Public Key: G,R - RSA Private Key: G,R - EC Public Key: G,R - EC Private Key: G,R - ML-KEM Public Key: G,R - ML-KEM Private Key: G,R - EDDSA Private Key: G,R - EDDSA Public Key: G,R - Intermediate Key Generation

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Value: G,E,Z
Key Verification	Verifying the public key	1	Public key	Success/ error	Key Verification with ECDSA	Crypto Officer - EC Public Key: W,E
Signature Generation	Generating signature	1	Message, EC private key or RSA private key, hash algorithm	Digital signature	Signature Generation with RSA Signature Generation with ECDSA	Crypto Officer - RSA Private Key: W,E - EC Private Key: W,E
Signature Verification	Verifying signature	1	Signature, EC public key or RSA public key, hash algorithm	Digital signature verification result	Signature Verification with ECDSA Signature Verification with RSA	Crypto Officer - RSA Public Key: W,E - EC Public Key: W,E
Shared Secret Computation	Calculating the Shared Secret	1	EC public key, EC private key	Shared Secret	Shared Secret Computation with EC Diffie-Hellman	Crypto Officer - EC Public Key: W,E - EC Private Key: W,E - Shared Secret: G,R
Key Derivation with TLS KDF	Deriving Keys	1	TLS Pre-Master Secret, key length	TLS Derived Key (AES/HMAC)	Key Derivation with TLS KDF	Crypto Officer - TLS Pre-Master Secret: W,E - TLS Master Secret: G,E,Z - TLS Derived Key (AES/HMAC): G,R
Key Derivation with PBKDF	Deriving Keys	1	Password, salt, iteration count, key length	PBKDF Derived Key	Key Derivation with PBKDF	Crypto Officer - PBKDF Derived Key: G,R - Password: W,E
Key Derivation	Deriving Keys	1	Shared Secret,	HKDF Derived Key	Key Derivation with KDA HKDF	Crypto Officer - HKDF

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
with KDA HKDF			Key Length			Derived Key: G,R - Shared Secret: W,E
Key Derivation with SSH KDF	Deriving Keys	1	Shared Secret, Key Length	SSH Derived Key	Key Derivation with SSH KDF	Crypto Officer - Shared Secret: W,E - SSH Derived Key: G,R
Key Derivation with KBKDF	Deriving Keys	1	Key Derivation Key	KBKDF Derived Key	Key Derivation with KBKDF	Crypto Officer - KBKDF Derived Key: G,R - Key Derivation Key: W,E
Key Derivation with KDA OneStep KDF	Deriving Keys	1	Shared Secret	KDA OneStep Derived Key	Key Derivation with KDA OneStep	Crypto Officer - Shared Secret: W,E - KDA OneStep Derived Key: G,R
Encapsulation	Encapsulation	1	ML-KEM Public Key	Ciphertext, ML-KEM Shared Secret	Encapsulation/Decapsulation with ML-KEM	Crypto Officer - ML-KEM Shared Secret: G,R,E - ML-KEM Public Key: W,E
Decapsulation	Decapsulation	1	ML-KEM Private Key, Ciphertext	ML-KEM Shared Secret	Encapsulation/Decapsulation with ML-KEM	Crypto Officer - ML-KEM Shared Secret: G,R - ML-KEM Private Key: W,E
Zeroization	Zeroize SSP in volatile memory	N/A	SSP	N/A	None	Crypto Officer - AES Key: Z - HMAC Key: Z - Entropy Input: Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - DRBG Internal State (V, Key): Z - RSA Public Key: Z - RSA Private Key: Z - EC Public Key: Z - EC Private Key: Z - Shared Secret: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Derived Key (AES/HMAC): Z - HKDF Derived Key: Z - SSH Derived Key: Z - PBKDF Derived Key: Z - Password: Z - Key Derivation Key: Z - KDA OneStep Derived Key: Z - KBKDF Derived Key: Z - ML-KEM Public Key: Z - ML-KEM Private Key: Z - EDDSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - EDDSA Public Key: Z - ML-KEM Shared Secret: Z - Intermediate Key Generation Value: Z
Show Status	Show status of the module state	N/A	N/A	Module status	None	Crypto Officer
Show Version	Show the version of the module using awslc_version_string	N/A	N/A	Module name and version	None	Crypto Officer
On-Demand Self-test	Initiate cryptographic algorithms self-tests and integrity test on-demand.	N/A	N/A	Pass or fail	Shared Secret Computation with EC Diffie-Hellman Key Wrapping/Unwrapping with AES KW, AES-KWP Key Wrapping/Unwrapping with AES GCM Key Wrapping/Unwrapping with AES CCM Encryption/Decryption with AES Signature Generation with RSA Signature Generation with ECDSA Signature Generation with EDDSA Key Generation with RSA Key Generation with ECDSA Key Generation with EDDSA Key Generation with ML-KEM Signature Verification with ECDSA Signature Verification with EDDSA Signature Verification with RSA Key Verification with ECDSA Encapsulation/Decapsulation with ML-KEM Key Derivation with TLS	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KDF Key Derivation with SSH KDF Key Derivation with KDA HKDF Key Derivation with KDA OneStep Key Derivation with PBKDF Key Derivation with KBKDF Message Digest with SHA Message Digest with SHAKE Random Number Generation with DRBG Message Authentication Generation with HMAC Message Authentication Generation with AES Authenticated Encryption/Decryption with AES CCM Authenticated Encryption/Decryption with AES GCM	

Table 12: Approved Services

For the above table, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

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

For the role, CO indicates “Crypto Officer”.

The module implements a service indicator that indicates whether the invoked service is approved. The service indicator is a return value 1 from the FIPS_service_indicator_check_approved function. This function is used together with two other functions. The usage is as follows:

- STEP 1: Should be called before invoking the service.

  int before = FIPS_service_indicator_before_call();
- STEP 2: Make a service call i.e., API function for performing a service.

  Func();
- STEP 3: Should be called after invoking the service.

  int after = FIPS_service_indicator_after_call();
- STEP 4: Return value 1 indicates approved service was invoked.

```
int ret = FIPS_service_indicator_check_approved(before, after);
```

Alternatively, all the above steps can be done by using a single call using the function CALL_SERVICE_AND_CHECK_APPROVED(approved, func).

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encryption	AES with OFB or CFB1, CFB8, CFB128 modes AES GCM, GCM, GMAC, XTS with keys not listed in Table 5 AES using aes_*_generic function RSA encryption primitive with PKCS#1 v1.5 and OAEP padding AES GMAC using aes_*_generic	CO
Decryption	Decryption	AES with OFB or CFB1, CFB8, CFB128 modes AES GCM, GCM, GMAC, XTS with keys not listed in Table 5 AES using aes_*_generic function AES GMAC using aes_*_generic	CO
Message Authentication Generation	MAC computation	AES using aes_*_generic function HMAC-MD4, HMAC-MD5, HMAC-SHA-3, HMAC-RIPEMD-160	CO
Message Digest	Generating message digest	MD4 MD5 (outside of TLS) RIPEMD-160	CO
Signature Generation	Generating signatures	RSA using keys less than 2048 bits RSA without hashing SHA-1	CO
Signature Verification	Verifying signatures	RSA using keys less than 1024 bits RSA without hashing	CO
Key Generation	Generating key pair	RSA using RSA_generate_key_ex ECDSA using EC_KEY_generate_key	CO
Shared Secret Computation	Calculating shared secret	Curve secp256k1 Diffie Hellman	CO
Key Derivation	Deriving TLS keys	TLS KDF using any SHA algorithms other than SHA2-256, SHA2-384, SHA2-512; or TLS KDF using non-extended master secret	CO
Key Encapsulation	Encrypting a key	RSA	CO
Key Un-encapsulation	Decrypting a key	RSA	CO

Table 13: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support loading of external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing a HMAC value calculated at run time on the bcm.o file, with the HMAC-SHA2-256 value stored within the module that was computed at build time.

5.2 Initiate on Demand

The module provides on-demand integrity test. The integrity test can be performed on demand by reloading the module. Additionally, the integrity test can be performed using the On-Demand Integrity Test service, which calls the BORINGSSL_integrity_test function.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module should be compiled and installed as stated in section 11. The user should confirm that the module is installed correctly by following steps 4 and 5 listed in section 11.

6.2 Configuration Settings and Restrictions

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

7 Physical Security

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

8 Non-Invasive Security

8.1 Mitigation Techniques

The module claims no non-invasive security techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 14: Storage Areas

9.2 SSP Input-Output Methods

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

Table 15: SSP Input-Output Methods

The module does not support entry and output of SSPs beyond the physical perimeter of the operational environment. The SSPs are provided to the module via API input parameters in the plaintext form and output via API output parameters in the plaintext form to and from the calling application running on the same operational environment.

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 zeros, which renders the SSP values irretrievable. The successful completion of the zeroization routine indicates that the zeroization procedure succeeded.	By calling the appropriate zeroization functions: OpenSSL_cleanse, EVP_CIPHER_CTX_cleanup, EVP_AEAD_CTX_zero, HMAC_CTX_cleanup, CTR_DRBG_clear, RSA_free, EC_KEY_free, KEM_KEY_free, EVP_PKEY_free
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed. The successful completion of the removal of power from the module indicates that zeroization has completed.	By unloading and reloading the module.
Automatically	Automatically zeroized when no longer needed	Memory occupied by SSPs is overwritten with zeros, which renders the SSP values irretrievable. The	N/A

Zeroization Method	Description	Rationale	Operator Initiation
		successful completion of the running service indicates that zeroization has completed.	

Table 16: SSP Zeroization Methods

All data output via the data output interface is inhibited when the module is performing zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES key used for encryption, decryption, and computing MAC tags	128-256 bits - 128-256 bits	Symmetric key - CSP			Key Wrapping/Unwrapping with AES KW, AES-KWP Key Wrapping/Unwrapping with AES GCM Key Wrapping/Unwrapping with AES CCM Encryption/Decryption with AES Message Authentication Generation with AES Authenticated Encryption/Decryption with AES CCM Authenticated Encryption/Decryption with AES GCM
HMAC Key	HMAC key for Message Authentication Generation	112-524288 bits - 112-256 bits	Authentication key - CSP			Message Authentication Generation with HMAC
Entropy Input	(IG D.L) Entropy input used to seed the DRBGs	256 bits - 256 bits	Entropy - CSP			Random Number Generation with DRBG
DRBG Seed	(IG D.L) DRBG seed derived from entropy input as defined in SP 800-90Ar1	256 bits - 256 bits	DRBG seed - CSP	Random Number Generation with DRBG		Random Number Generation with DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State (V, Key)	(IG D.L) Internal state of CTR_DRBG	V: 128 bits, Key: 256 bits - 256 bits	Internal state - CSP	Random Number Generation with DRBG		Random Number Generation with DRBG
RSA Public Key	RSA public key used for RSA key generation, signature verification	1024, 2048, 3072, 4096 bits - 80-150 bits	Public key - PSP	Key Generation with RSA		Signature Verification with RSA
RSA Private Key	RSA private key used for RSA key generation, signature generation	2048, 3072, 4096 bits - 112-150 bits	Private key - CSP	Key Generation with RSA		Signature Generation with RSA
EC Public Key	EC public key used for EC key generation, key verification, signature verification, shared secret computation	P-224, P-256, P-384, P-521 - 112-256 bits	Public key - PSP	Key Generation with ECDSA		Shared Secret Computation with EC Diffie-Hellman Signature Verification with ECDSA Key Verification with ECDSA
EC Private Key	EC private key used for EC key generation, key verification, signature generation, shared secret computation	P-224, P-256, P-384, P-521 - 112-256 bits	Private key - CSP	Key Generation with ECDSA		Shared Secret Computation with EC Diffie-Hellman Signature Generation with ECDSA
ML-KEM Public Key	ML-KEM public key used for ML-KEM key generation, ML-KEM Key Encapsulation	800, 1184, 1568 bytes - 128-256 bits	Public key - PSP	Key Generation with ML-KEM		Encapsulation/Decapsulation with ML-KEM

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ML-KEM Private Key	ML-KEM private key used for ML-KEM key generation, ML-KEM Key Decapsulation	1632, 2400, 3168 bytes - 128-256 bits	Private key - CSP	Key Generation with ML-KEM		Encapsulation/Decapsulation with ML-KEM
EDDSA Private Key	EDDSA private key used for EDDSA key generation, signature generation	256 bits - 128 bits	Private key - CSP	Key Generation with EDDSA		Signature Generation with EDDSA
EDDSA Public Key	EDDSA public key used for EDDSA key generation, signature verification	256 bits - 128 bits	Public key - PSP	Key Generation with EDDSA		Signature Verification with EDDSA
Shared Secret	Shared secret established with KAS-SSC	P-224, P-256, P-384, P-521 - 112-256 bits	Shared secret - CSP		Shared Secret Computation with EC Diffie-Hellman	Key Derivation with TLS KDF Key Derivation with SSH KDF Key Derivation with KDA HKDF
ML-KEM Shared Secret	Shared secret established with ML-KEM	32 bytes - 128-256 bits	Shared secret - CSP		Encapsulation/Decapsulation with ML-KEM	
TLS Pre-Master Secret	TLS Pre-Master secret used for deriving the TLS Master Secret	P-224, P-256, P-384, P-521 - 112-256 bits	TLS pre-master secret - CSP			Key Derivation with TLS KDF Key Derivation with KDA HKDF
TLS Master Secret	TLS Master secret used for deriving the TLS Derived Key	384 bits - 112-256 bits	TLS master secret - CSP	Key Derivation with TLS KDF Key Derivation with KDA HKDF		Key Derivation with TLS KDF Key Derivation with KDA HKDF
TLS Derived Key	TLS Derived Key from	AES: 128-256 bits	Symmetric key - CSP	Key Derivatio		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
(AES/HMAC)	TLS Master Secret	HMAC: 112 to 256 bits - AES: 128-256 bits HMAC: 112 to 256 bits		n with TLS KDF		
HKDF Derived Key	KDA HKDF derived key	2048 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with KDA HKDF		
SSH Derived Key	SSH KDF derived key	128 to 512 bits - 112 to 256 bits	Symmetric key - CSP	Key Derivation with SSH KDF		
PBKDF Derived Key	PBKDF derived key	128 to 4096 bits - N/A	Symmetric key - CSP	Key Derivation with PBKDF		
KBKDF Derived Key	KBKDF derived key	2048 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with KBKDF		
Password	Password for PBKDF	14-128 characters - N/A	Password - CSP			Key Derivation with PBKDF
Key Derivation Key	Key derivation key	112-524288 bits - 112-256 bits	Symmetric key - CSP			Key Derivation with KBKDF
KDA OneStep Derived Key	KDA OneStep derived key	2048 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with KDA OneStep		
Intermediate Key Generation Value	Intermediate key generation value	224-4096 bits - 112-256 bits	Intermediate value - CSP	Key Generation with RSA Key Generation with ECDSA		Key Generation with RSA Key Generation with ECDSA

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	
HMAC Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	
Entropy Input	API input parameters	RAM:Plaintext	From service invocation to service completion	Module Reset Automatically	DRBG Seed:Generation OF
DRBG Seed		RAM:Plaintext	From service invocation to service completion	Module Reset Automatically	Entropy Input:Derived From DRBG Internal State (V, Key):Generation Of
DRBG Internal State (V, Key)		RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	DRBG Seed:Derived From
RSA Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	RSA Private Key:Paired With Intermediate Key Generation Value:Generated From
RSA Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	RSA Public Key:Paired With Intermediate Key Generation Value:Generated From
EC Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	EC Private Key:Paired With Shared Secret:Generation Of Intermediate Key Generation Value:Generated From
EC Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	EC Public Key:Paired With Shared Secret:Generation Of Intermediate Key Generation Value:Generated From
ML-KEM Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	ML-KEM Private Key:Paired With ML-KEM Shared Secret:Encapsulates Intermediate Key Generation Value:Generated From
ML-KEM Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	ML-KEM Public Key:Paired With ML-KEM Shared Secret:Decapsulates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Intermediate Key Generation Value:Generated From
EDDSA Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	EDDSA Public Key:Paired With Intermediate Key Generation Value:Generated From
EDDSA Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	EDDSA Private Key:Paired With Intermediate Key Generation Value:Generated From
Shared Secret	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	EC Public Key:Derived From EC Private Key:Derived From
ML-KEM Shared Secret	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	ML-KEM Public Key:Encapsulated With ML-KEM Private Key:Decapsulated With
TLS Pre-Master Secret	API input parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	TLS Master Secret:Derivation Of
TLS Master Secret		RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	TLS Pre-Master Secret:Derived From TLS Derived Key (AES/HMAC):Derivation Of
TLS Derived Key (AES/HMAC)	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	TLS Master Secret:Derived From
HKDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	Shared Secret:Derived From
SSH Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	Shared Secret:Derived From
PBKDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	Password:Derived From
KBKDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	Key Derivation Key:Derived From
Password	API input parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	PBKDF Derived Key:Derivation Of

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Key Derivation Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	KBKDF Derived Key:Derivation Of
KDA OneStep Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Free Cipher Handle Module Reset	Shared Secret:Derived From
Intermediate Key Generation Value		RAM:Plaintext	From service invocation to service completion	Module Reset Automatically	RSA Public Key:Generation Of RSA Private Key:Generation Of EC Public Key:Generation Of EC Private Key:Generation Of ML-KEM Public Key:Generation Of ML-KEM Private Key:Generation Of EDDSA Private Key:Generation Of EDDSA Public Key:Generation Of

Table 18: SSP Table 2

9.5 Transitions

The SHA-1 algorithm as implemented by the module will be non-approved for all purposes, starting January 1, 2030.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A6288)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A6289)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A6291)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A6295)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A6312)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A6315)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o

Table 19: Pre-Operational Self-Tests

The module performs the pre-operational self-test automatically when the module is loaded into memory; the pre-operational self-test is the software integrity test that ensures that the module is not corrupted. While the module is executing the pre-operational self-test, services are not available, and input and output are inhibited.

The software integrity test is performed after a set of conditional cryptographic algorithm self-tests (CASTs). The set of CASTs executed before the software integrity test consists of HMAC-SHA2-256 KAT, which is used in the pre-operational self-test, and the SHA2-256 KAT.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A6283)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6286)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6292)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6296)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6301)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6306)	Encrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A6283)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6286)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6292)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6296)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6301)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-CBC (A6306)	Decrypt with 128-bit key	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6284)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6285)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6287)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6293)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6297)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6298)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6299)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6300)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6302)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6303)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6304)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A6305)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6307)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6308)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6309)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6310)	Encrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6284)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6285)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6287)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6293)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6297)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6298)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6299)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6300)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6302)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6303)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6304)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6305)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A6307)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6308)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6309)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
AES-GCM (A6310)	Decrypt with 128-bit key, 96-bit (internal IV)	KAT	CAST	Module becomes operational	Symmetric operation	Module power-on
SHA-1 (A6288)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6289)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6291)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6295)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6312)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6313)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6314)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA-1 (A6315)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6288)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6289)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6291)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6295)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6312)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A6313)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6314)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-256 (A6315)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6288)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6289)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6291)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6295)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6312)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6313)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6314)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA2-512 (A6315)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
SHA3-256 (A6294)	128-bit message	KAT	CAST	Module becomes operational	Message digest	Module power-on
HMAC-SHA2-256 (A6288)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6289)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6291)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6295)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6312)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A6313)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6314)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
HMAC-SHA2-256 (A6315)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on
Counter DRBG (A6283)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
Counter DRBG (A6286)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
Counter DRBG (A6292)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
Counter DRBG (A6296)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
Counter DRBG (A6301)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
Counter DRBG (A6306)	256 bit keys, DF, without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Module power-on
ECDSA SigGen (FIPS186-5) (A6288)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6289)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6291)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6295)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-5) (A6312)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6313)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6314)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigGen (FIPS186-5) (A6315)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6288)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6289)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6291)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6295)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6312)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A6313)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6314)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
ECDSA SigVer (FIPS186-5) (A6315)	SHA2-256 with P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification or shared secret computation services
EDDSA SigGen (A6288)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6289)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6291)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6295)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6312)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6313)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigGen (A6314)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
EDDSA SigGen (A6315)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6288)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6289)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6291)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6295)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6312)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6313)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6314)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
EDDSA SigVer (A6315)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6288)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6289)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification services
RSA SigGen (FIPS186-5) (A6290)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6291)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6295)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6312)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6313)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6314)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigGen (FIPS186-5) (A6315)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6288)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6289)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6290)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-5) (A6291)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6295)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6312)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6313)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6314)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
RSA SigVer (FIPS186-5) (A6315)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation or signature verification services
KAS-ECC-SSC Sp800-56Ar3 (A6288)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6289)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6291)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6295)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-ECC-SSC Sp800-56Ar3 (A6312)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6313)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6314)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KAS-ECC-SSC Sp800-56Ar3 (A6315)	P-256 curve	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
KDF SP800-108 (A6288)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6289)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6291)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6295)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6312)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6313)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6314)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDF SP800-108 (A6315)	HMAC-SHA2-256	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6288)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDA OneStep SP800-56Cr2 (A6289)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6291)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6295)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6312)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6313)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6314)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA OneStep SP800-56Cr2 (A6315)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6288)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6289)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6291)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6295)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6312)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6313)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6314)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
KDA HKDF Sp800-56Cr1 (A6315)	SHA2-256	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on
PBKDF (A6288)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6289)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
PBKDF (A6291)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6295)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6312)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6313)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6314)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
PBKDF (A6315)	SHA2-256	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on
ECDSA KeyGen (FIPS186-5) (A6288)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6289)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6291)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6295)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6312)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6313)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6314)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6315)	SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6288)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA KeyGen (FIPS186-5) (A6289)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6290)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6291)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6295)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6312)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6313)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6314)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6315)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ML-KEM KeyGen (A6288)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6289)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6291)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6295)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6312)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6313)	(800, 1632) byte keys; KeyGen encapsulate;	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	KeyGen decapsulate					decapsulation services
ML-KEM KeyGen (A6314)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen (A6315)	(800, 1632) byte keys; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6288)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6289)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6291)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6295)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6312)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6313)	(800, 1632) byte keys; Encapsulate ciphertext; Encapsulate shared secret	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6314)	(800, 1632) byte keys; Decapsulate non-rejection; Decapsulate implicit rejection	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A6315)	(800, 1632) byte keys; Decapsulate non-rejection; Decapsulate implicit rejection	KAT	CAST	Module becomes operational	Encapsulation and Decapsulation	First usage of key pair generation, encapsulation or decapsulation services

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ML-KEM KeyGen (A6288)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6289)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6291)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6295)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6312)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6313)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6314)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
ML-KEM KeyGen (A6315)	32-bytes shared secret	PCT	PCT	Successful key pair generation	Encapsulation and Decapsulation	Key pair generation
KDF TLS (A6288)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6289)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6291)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6295)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6312)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6313)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6314)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
KDF TLS (A6315)	SHA2-256	KAT	CAST	Module becomes operational	Key derivation	Module power-on
EDDSA KeyGen (A6288)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
EDDSA KeyGen (A6289)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6291)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6295)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6312)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6313)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6314)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A6315)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Table 20: Conditional Self-Tests

Conditional Cryptographic Algorithm Tests

The module performs self-tests on approved cryptographic algorithms, using the tests shown in the *Conditional Self-Tests* table. Data output through the data output interface is inhibited during the self-tests. The CASTs are performed in the form of Known Answer Tests (KATs), in which the calculated output is compared with the expected known answer (that are hard-coded in the module). A failed match causes a failure of the self-test. If any of these self-tests fails, the module transitions to error state.

Conditional Pair-Wise Consistency Tests

The module implements RSA, ECDSA, EDDSA key generation services and performs the respective pairwise consistency test (PCT) using sign and verify functions. Additionally, the module performs ML-KEM key generation service and performs the PCT using encapsulation and decapsulation. The PCTs are listed in the *Conditional Self-Tests* table. If any of these self-tests fails, the module transitions to error state and is aborted.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6288)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A6289)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A6291)	Message Authentication	SW/FW Integrity	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6295)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A6312)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A6315)	Message Authentication	SW/FW Integrity	On demand	Manually

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A6283)	KAT	CAST	On Demand	Manually
AES-CBC (A6286)	KAT	CAST	On Demand	Manually
AES-CBC (A6292)	KAT	CAST	On Demand	Manually
AES-CBC (A6296)	KAT	CAST	On Demand	Manually
AES-CBC (A6301)	KAT	CAST	On Demand	Manually
AES-CBC (A6306)	KAT	CAST	On Demand	Manually
AES-CBC (A6283)	KAT	CAST	On Demand	Manually
AES-CBC (A6286)	KAT	CAST	On Demand	Manually
AES-CBC (A6292)	KAT	CAST	On Demand	Manually
AES-CBC (A6296)	KAT	CAST	On Demand	Manually
AES-CBC (A6301)	KAT	CAST	On Demand	Manually
AES-CBC (A6306)	KAT	CAST	On Demand	Manually
AES-GCM (A6284)	KAT	CAST	On Demand	Manually
AES-GCM (A6285)	KAT	CAST	On Demand	Manually
AES-GCM (A6287)	KAT	CAST	On Demand	Manually
AES-GCM (A6293)	KAT	CAST	On Demand	Manually
AES-GCM (A6297)	KAT	CAST	On Demand	Manually
AES-GCM (A6298)	KAT	CAST	On Demand	Manually
AES-GCM (A6299)	KAT	CAST	On Demand	Manually
AES-GCM (A6300)	KAT	CAST	On Demand	Manually
AES-GCM (A6302)	KAT	CAST	On Demand	Manually
AES-GCM (A6303)	KAT	CAST	On Demand	Manually
AES-GCM (A6304)	KAT	CAST	On Demand	Manually
AES-GCM (A6305)	KAT	CAST	On Demand	Manually
AES-GCM (A6307)	KAT	CAST	On Demand	Manually
AES-GCM (A6308)	KAT	CAST	On Demand	Manually
AES-GCM (A6309)	KAT	CAST	On Demand	Manually
AES-GCM (A6310)	KAT	CAST	On Demand	Manually
AES-GCM (A6284)	KAT	CAST	On Demand	Manually
AES-GCM (A6285)	KAT	CAST	On Demand	Manually
AES-GCM (A6287)	KAT	CAST	On Demand	Manually
AES-GCM (A6293)	KAT	CAST	On Demand	Manually
AES-GCM (A6297)	KAT	CAST	On Demand	Manually
AES-GCM (A6298)	KAT	CAST	On Demand	Manually
AES-GCM (A6299)	KAT	CAST	On Demand	Manually
AES-GCM (A6300)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A6302)	KAT	CAST	On Demand	Manually
AES-GCM (A6303)	KAT	CAST	On Demand	Manually
AES-GCM (A6304)	KAT	CAST	On Demand	Manually
AES-GCM (A6305)	KAT	CAST	On Demand	Manually
AES-GCM (A6307)	KAT	CAST	On Demand	Manually
AES-GCM (A6308)	KAT	CAST	On Demand	Manually
AES-GCM (A6309)	KAT	CAST	On Demand	Manually
AES-GCM (A6310)	KAT	CAST	On Demand	Manually
SHA-1 (A6288)	KAT	CAST	On Demand	Manually
SHA-1 (A6289)	KAT	CAST	On Demand	Manually
SHA-1 (A6291)	KAT	CAST	On Demand	Manually
SHA-1 (A6295)	KAT	CAST	On Demand	Manually
SHA-1 (A6312)	KAT	CAST	On Demand	Manually
SHA-1 (A6313)	KAT	CAST	On Demand	Manually
SHA-1 (A6314)	KAT	CAST	On Demand	Manually
SHA-1 (A6315)	KAT	CAST	On Demand	Manually
SHA2-256 (A6288)	KAT	CAST	On Demand	Manually
SHA2-256 (A6289)	KAT	CAST	On Demand	Manually
SHA2-256 (A6291)	KAT	CAST	On Demand	Manually
SHA2-256 (A6295)	KAT	CAST	On Demand	Manually
SHA2-256 (A6312)	KAT	CAST	On Demand	Manually
SHA2-256 (A6313)	KAT	CAST	On Demand	Manually
SHA2-256 (A6314)	KAT	CAST	On Demand	Manually
SHA2-256 (A6315)	KAT	CAST	On Demand	Manually
SHA2-512 (A6288)	KAT	CAST	On Demand	Manually
SHA2-512 (A6289)	KAT	CAST	On Demand	Manually
SHA2-512 (A6291)	KAT	CAST	On Demand	Manually
SHA2-512 (A6295)	KAT	CAST	On Demand	Manually
SHA2-512 (A6312)	KAT	CAST	On Demand	Manually
SHA2-512 (A6313)	KAT	CAST	On Demand	Manually
SHA2-512 (A6314)	KAT	CAST	On Demand	Manually
SHA2-512 (A6315)	KAT	CAST	On Demand	Manually
SHA3-256 (A6294)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6288)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6289)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6291)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6295)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6312)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6313)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6314)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6315)	KAT	CAST	On Demand	Manually
Counter DRBG (A6283)	KAT	CAST	On Demand	Manually
Counter DRBG (A6286)	KAT	CAST	On Demand	Manually
Counter DRBG (A6292)	KAT	CAST	On Demand	Manually
Counter DRBG (A6296)	KAT	CAST	On Demand	Manually
Counter DRBG (A6301)	KAT	CAST	On Demand	Manually
Counter DRBG (A6306)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6288)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6289)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6291)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6295)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6312)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6313)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6314)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6315)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6288)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6289)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6291)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6295)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A6312)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6313)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6314)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6315)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6288)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6289)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6291)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6295)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6312)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6313)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6314)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A6315)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6288)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6289)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6291)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6295)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6312)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6313)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6314)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A6315)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6288)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6289)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-5) (A6290)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6291)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6295)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6312)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6313)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6314)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A6315)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6288)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6289)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6290)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6291)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6295)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6312)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6313)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6314)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A6315)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6288)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A6289)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6291)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6295)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6312)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6313)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6314)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6315)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6288)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6289)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6291)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6295)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6312)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6313)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6314)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A6315)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6288)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6289)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6291)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6295)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6312)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA OneStep SP800-56Cr2 (A6313)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6314)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A6315)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6288)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6289)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6291)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6295)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6312)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6313)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6314)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A6315)	KAT	CAST	On Demand	Manually
PBKDF (A6288)	KAT	CAST	On Demand	Manually
PBKDF (A6289)	KAT	CAST	On Demand	Manually
PBKDF (A6291)	KAT	CAST	On Demand	Manually
PBKDF (A6295)	KAT	CAST	On Demand	Manually
PBKDF (A6312)	KAT	CAST	On Demand	Manually
PBKDF (A6313)	KAT	CAST	On Demand	Manually
PBKDF (A6314)	KAT	CAST	On Demand	Manually
PBKDF (A6315)	KAT	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6288)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6289)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6291)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6295)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6312)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6313)	PCT	PCT	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) (A6314)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6315)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6288)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6289)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6290)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6291)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6295)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6312)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6313)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6314)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A6315)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6288)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6289)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6291)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6295)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6312)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6313)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6314)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6315)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6288)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ML-KEM EncapDecap (A6289)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6291)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6295)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6312)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6313)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6314)	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A6315)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen (A6288)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6289)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6291)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6295)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6312)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6313)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6314)	PCT	PCT	On Demand	Manually
ML-KEM KeyGen (A6315)	PCT	PCT	On Demand	Manually
KDF TLS (A6288)	KAT	CAST	On Demand	Manually
KDF TLS (A6289)	KAT	CAST	On Demand	Manually
KDF TLS (A6291)	KAT	CAST	On Demand	Manually
KDF TLS (A6295)	KAT	CAST	On Demand	Manually
KDF TLS (A6312)	KAT	CAST	On Demand	Manually
KDF TLS (A6313)	KAT	CAST	On Demand	Manually
KDF TLS (A6314)	KAT	CAST	On Demand	Manually
KDF TLS (A6315)	KAT	CAST	On Demand	Manually
EDDSA KeyGen (A6288)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6289)	PCT	PCT	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
EDDSA KeyGen (A6291)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6295)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6312)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6313)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6314)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A6315)	PCT	PCT	On Demand	Manually

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The library is aborted with SIGABRT signal. Module is no longer operational the data output interface is inhibited	Pre-operational test failure; CAST failure; PCT failure	Module reset	An error message is output on the stderr and then the module is aborted.

Table 23: Error States

If the module fails any of the self-tests, the module enters an error state. To recover from any error state, the module must be rebooted.

10.5 Operator Initiation of Self-Tests

The software integrity tests and the CASTs for HMAC, SHA, AES, DRBG, TLS KDF, PBKDF2, KDA OneStep, KBKDF, KDA HKDF, can be invoked by unloading and subsequently re-initializing the module. The CASTs for ECDSA, EDDSA, RSA can be invoked by requesting the corresponding Key Generation, Digital Signature Generation, Digital Signature Verification services. The CAST for KAS-ECC-SSC can be invoked by requesting the Shared Secret Computation service. The CASTs for ML-KEM can be invoked by the corresponding Key Generation, Encapsulation and Decapsulation services. Additionally, all the CASTs can be invoked by calling the BORINGSSL_self_test function. The PCTs can be invoked on demand by requesting the Key Generation service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module bcm.o is embedded into the usersapce application which can be obtained by building the source code at the following location [1]. The set of files specified in the archive constitutes the complete set of source files of the validated module. There shall be no additions, deletions, or alterations of this set as used during module build.

[1] https://github.com/aws/aws-lc/tree/fips-2024-09-27

The downloaded zip file can be verified by issuing the “sha256sum aws-lc-fips-2024-09-27.zip” command. The expected SHA2-256 digest value is:

d543f4efde2130b966ef4fff468f17ad212a8ef6bdc93199c9fe34ecf925030d

After the zip file is extracted, the instructions listed below will compile the module. The compilation instructions must be executed separately on platforms that have different processors and/or operating systems. Due to two possible combinations of OS/processor, the module count is two (i.e., there are two separate binaries generated, one for each entry listed in the *Tested Operational Environments* table).

Amazon Linux 2023:

1. `sudo yum groupinstall "Development Tools"`
2. `sudo yum install cmake3 golang`
3. `cd aws-lc-fips-2024-09-27`
4. `mkdir build`
5. `cd build`
6. `cmake3 -DFIPS=1 ..`
7. `make`

Upon completion of the build process, the module’s status can be verified by the command below. If the value obtained is “1” then the module has been installed and configured to operate in FIPS compliant manner.

```
./tool/bssl isfips
```

Lastly, the user can call the “show version” service using awslc_version_string function and the expected output is “AWS-LC FIPS 3.0.0” which is the module version. This will confirm that the module is in the operational mode. Additionally, the “AWS-LC FIPS” also acts as the module identifier and the verification of the "static" part can be done using following command with an application that was used for static linking. The "T" in the output confirms that the module is statically linked.

Command: *nm <application_name> | grep awslc_version_string*

Example Output: *0000000000a5bdff **T** awslc_version_string*

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.

When the module is at end of life, for the GitHub repo, the README will be modified to mark the library as deprecated. After a 6-month window, more restrictive branch permissions will be added such that only administrators can read from the FIPS branch.

The module does not possess persistent storage of SSPs. The SSP value only exists in volatile memory and that value vanishes when the module is powered off. So as a first step for the secure sanitization, the module needs to be powered off. Then for actual deprecation, the module will be upgraded to newer version that is approved. This upgrade process will uninstall/remove the old/terminated module and provide a new replacement.

12 Mitigation of Other Attacks

12.1 Attack List

RSA timing attacks.

12.2 Mitigation Effectiveness

RSA is vulnerable to timing attacks. In a setup where attackers can measure the time of RSA decryption or signature operations, blinding must be used to protect the RSA operation from that attack.

The module provides the mechanism to use the blinding for RSA. When the blinding is on, the module generates a random value to form a blinding factor in the RSA key before the RSA key is used in the RSA cryptographic operations.