

Amazon Web Services, Inc.

AWS-LC 4 Cryptographic Module (dynamic)

FIPS 140-3 Non-Proprietary Security Policy

Document version: 1.5

Last update: 2026-11-02

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 10
2.6 Security Function Implementations 18
2.7 Algorithm Specific Information 28
2.8 RBG and Entropy 31
2.9 Key Generation 32
2.10 Key Establishment 32
2.11 Industry Protocols 32
3 Cryptographic Module Interfaces 33
3.1 Ports and Interfaces 33
4 Roles, Services, and Authentication 34
4.1 Authentication Methods 34
4.2 Roles 34
4.3 Approved Services 34
4.4 Non-Approved Services 47
4.5 External Software/Firmware Loaded 48
5 Software/Firmware Security 49
5.1 Integrity Techniques 49
5.2 Initiate on Demand 49
6 Operational Environment 50
6.1 Operational Environment Type and Requirements 50
6.2 Configuration Settings and Restrictions 50
7 Physical Security 51
8 Non-Invasive Security 52
8.1 Mitigation Techniques 52
9 Sensitive Security Parameters Management 53
9.1 Storage Areas 53
9.2 SSP Input-Output Methods 53
9.3 SSP Zeroization Methods 53
9.4 SSPs 54
9.5 Transitions 65

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests 67
10.1 Pre-Operational Self-Tests 67
10.2 Conditional Self-Tests 67
10.3 Periodic Self-Test Information 93
10.4 Error States 104
10.5 Operator Initiation of Self-Tests 105
11 Life-Cycle Assurance 106
11.1 Installation, Initialization, and Startup Procedures 106
11.2 Administrator Guidance 107
11.3 Non-Administrator Guidance 107
12 Mitigation of Other Attacks 108
12.1 Attack List 108
12.2 Mitigation Effectiveness 108

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 9
Table 4: Modes List and Description 9
Table 5: Approved Algorithms 16
Table 6: Vendor-Affirmed Algorithms 17
Table 7: Non-Approved, Allowed Algorithms with No Security Claimed 17
Table 8: Non-Approved, Not Allowed Algorithms 18
Table 9: Security Function Implementations 28
Table 10: Entropy Certificates 31
Table 11: Entropy Sources 32
Table 12: Ports and Interfaces 33
Table 13: Roles 34
Table 14: Approved Services 47
Table 15: Non-Approved Services 48
Table 16: Storage Areas 53
Table 17: SSP Input-Output Methods 53
Table 18: SSP Zeroization Methods 53
Table 19: SSP Table 1 59
Table 20: SSP Table 2 65
Table 21: Pre-Operational Self-Tests 67
Table 22: Conditional Self-Tests 92
Table 23: Pre-Operational Periodic Information 93
Table 24: Conditional Periodic Information 104
Table 25: Error States 104

List of Figures

Figure 1: Block Diagram 7

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version AWS-LC FIPS 4.0.0 of the AWS-LC 4 Cryptographic Module (dynamic). 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 4 Cryptographic Module (dynamic) 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,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The AWS-LC 4 Cryptographic Module (dynamic) (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: Multi-Chip Standalone

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 4 Cryptographic Module (dynamic) which is a cryptographic library consisting of the bcm.o file (version AWS-LC FIPS 4.0.0). This file is dynamically 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.

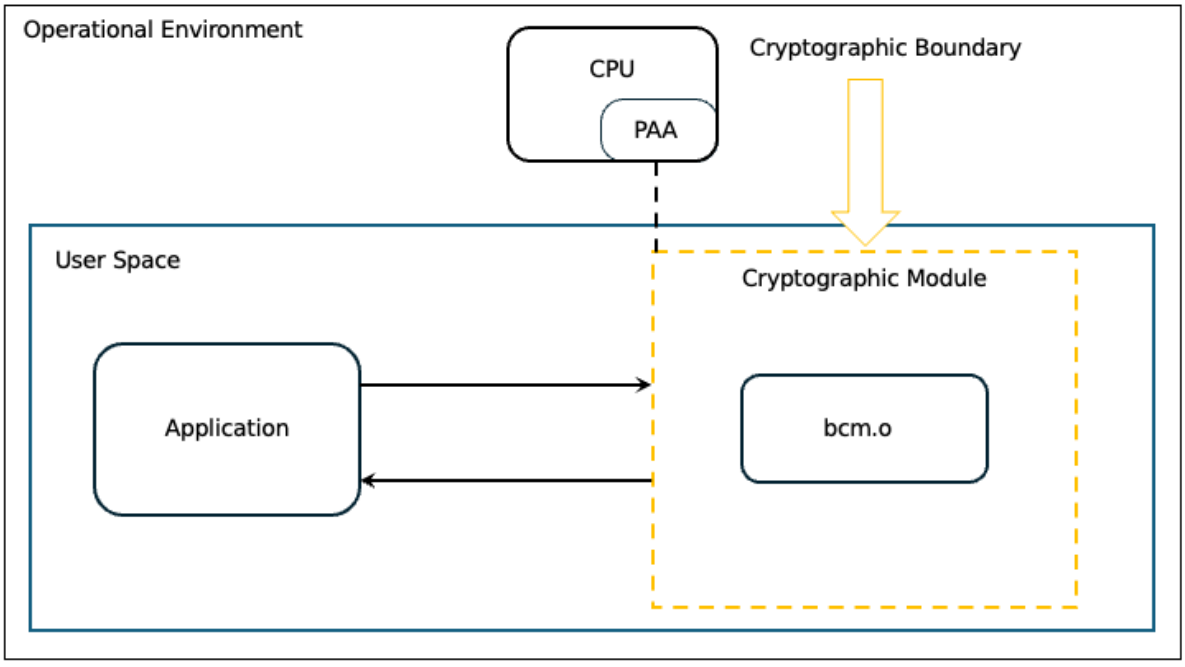


Figure 1: Block Diagram

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
bcm.o on Amazon Linux 2023 on Amazon EC2 c6i.metal with 192 GiB system memory and Elastic Block Store (EBS) 200 GiB with Intel(R) Xeon(R) Platinum 8375C	AWS-LC FIPS 4.0.0		HMAC-SHA2-256
bcm.o on Amazon Linux 2023 on Amazon EC2 r8g.metal-24xl with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB with Graviton4	AWS-LC FIPS 4.0.0		HMAC-SHA2-256
bcm.o on Amazon Linux 2023 on Amazon EC2 c7a.metal with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB with AMD EPYC 4th Generation	AWS-LC FIPS 4.0.0		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	Amazon EC2 c6i.metal with 192 GiB system memory and Elastic Block Store (EBS) 200 GiB	Intel(R) Xeon(R) Platinum 8375C	Yes	N/A	AWS-LC FIPS 4.0.0
Amazon Linux 2023	Amazon EC2 c6i.metal with 192 GiB system memory and Elastic Block Store (EBS) 200 GiB	Intel(R) Xeon(R) Platinum 8375C	No	N/A	AWS-LC FIPS 4.0.0
Amazon Linux 2023	Amazon EC2 r8g.metal-24xl with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB	Graviton4	Yes	N/A	AWS-LC FIPS 4.0.0
Amazon Linux 2023	Amazon EC2 r8g.metal-24xl with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB	Graviton4	No	N/A	AWS-LC FIPS 4.0.0

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Amazon Linux 2023	Amazon EC2 c7a.metal with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB	AMD EPYC 4th Generation	Yes	N/A	AWS-LC FIPS 4.0.0
Amazon Linux 2023	Amazon EC2 c7a.metal with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB	AMD EPYC 4th Generation	No	N/A	AWS-LC FIPS 4.0.0

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

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

N/A for this module.

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Return value 0 from the function: CALL_SERVICE_AND_CHECK_APPROVED()

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 a set of 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7839, A7844, A7849, A7860, A7866, A7869	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A7839, A7844, A7849, A7860, A7866, A7869	Key Length - 128 Tag Length - 32 IV Length - IV Length: 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CMAC	A7839, A7844, A7849, A7860, A7866, A7869	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 32-128 Increment 8 Message Length - Message Length: 0-65536 Increment 8	SP 800-38B
AES-CTR	A7839, A7844, A7849, A7860, A7866, A7869	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - Yes Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A7839, A7840, A7841, A7842, A7843, A7844, A7845, A7846, A7847, A7848, A7849, A7850, A7851, A7852, A7853, A7860, A7861, A7866, A7867, A7868, A7869, A7870	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853, A7861, A7867, A7868, A7870	Direction - Decrypt, Encrypt IV Generation - External, Internal Key Length - 128, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128-65536 Increment 128 AAD Length - AAD Length: 0-320 Increment 8 IV Generation Mode - 8.2.1, 8.2.2	SP 800-38D
AES-GMAC	A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853,	Direction - Decrypt, Encrypt IV Generation - External, Internal Key Length - 128, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 AAD Length - AAD Length: 0-320 Increment	SP 800-38D

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
	A7861, A7867, A7868, A7870	8 IV Generation Mode - 8.2.1, 8.2.2	
AES-KW	A7839, A7844, A7849, A7860, A7866, A7869	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-KWP	A7839, A7844, A7849, A7860, A7866, A7869	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 8-4096 Increment 8	SP 800-38F
AES-XTS Testing Revision 2.0	A7839, A7844, A7849, A7854, A7860, A7866, A7869	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A7839, A7844, A7849, A7860, A7866, A7869	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 256 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 384 Returned Bits - 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A7864	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A7855, A7856, A7857, A7858, A7859, A7863, A7864, A7871, A7872	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7855, A7862, A7865, A7871, A7874, A7875, A7876	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7856, A7857, A7858, A7859, A7863, A7872	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A7855, A7862, A7865, A7871, A7874, A7875, A7876	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-5)	A7856, A7857, A7858, A7859, A7863, A7872	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
EDDSA KeyGen	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Curve - ED-25519	FIPS 186-5
EDDSA SigGen	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Curve - ED-25519 Context Length - Context Length: 0 PreHash - Yes Pure - Yes	FIPS 186-5
EDDSA SigVer	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Curve - ED-25519 PreHash - Yes Pure - Yes	FIPS 186-5
HMAC-SHA-1	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 160 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	MAC - MAC: 224 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	MAC - MAC: 256 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-384	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	MAC - MAC: 384 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	MAC - MAC: 512 Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A7864	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Fixed Info Pattern - uPartyInfo||vPartyInfo||l Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-2048 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A7855, A7862, A7865, A7871, A7874, A7875, A7876	Auxiliary Function Methods - Auxiliary Function Name - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-2048 Increment 8	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A7856, A7857, A7858, A7859, A7863, A7872	Auxiliary Function Methods - Auxiliary Function Name - HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 MAC Salting Methods - default, random Fixed Info Pattern - uPartyInfo||vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-2048 Increment 8	SP 800-56C Rev. 2
KDF SP800-108	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	KDF Mode - Counter, Feedback MAC Mode - HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256 Supported Lengths - Supported Lengths: 2048 Fixed Data Order - After Fixed Data, Before Fixed Data Counter Length - 32, 8 Supports Empty IV - Yes Requires Empty IV - Yes Custom Key In Length - 0	SP 800-108 Rev. 1

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	TLS Version - v1.0/1.1, v1.2 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
ML-DSA KeyGen	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87	FIPS 204
ML-DSA SigGen	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Signature Interfaces - external, internal Pre Hash - pure Deterministic - No External Mu - No, Yes Key Formats - expanded Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Context Length - Context Length: 0-1024 Increment 8	FIPS 204
ML-DSA SigVer	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Signature Interfaces - external, internal Pre Hash - pure External Mu - No, Yes Parameter Sets - ML-DSA-44, ML-DSA-65, ML-DSA-87 Message Length - Message Length: 8-65536 Increment 8 Context Length - Context Length: 0-1024 Increment 8	FIPS 204
ML-KEM EncapDecap	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768 Functions - Decapsulation, Decapsulation Key Check, Encapsulation, Encapsulation Key Check	FIPS 203
ML-KEM KeyGen	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Parameter Sets - ML-KEM-1024, ML-KEM-512, ML-KEM-768	FIPS 203
PBKDF	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Iteration Count - Iteration Count: 1000-10000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Password Length - Password Length: 14-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A7864, A7873	Key Generation Mode - probable Modulo - 2048, 3072, 4096, 6144, 8192 p mod 8 - 0	FIPS 186-5

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Primality Tests - 2powSecStr q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - No Private Key Format - standard Public Exponent Mode - fixed	
RSA SigGen (FIPS186-5)	A7855, A7862, A7865, A7871, A7874, A7875, A7876	Hash Pair - Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Salt Length - 28, 32, 48, 64 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigGen (FIPS186-5)	A7856, A7857, A7858, A7859, A7863, A7872, A7873	Hash Pair - Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Salt Length - 28, 32, 48, 64 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-4)	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872, A7873	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Salt Length - 20, 28, 32, 48, 62 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA SigVer (FIPS186-5)	A7855, A7862, A7865, A7871, A7874, A7875, A7876	Hash Pair - Hash Algorithm - SHA3-224, SHA3-256, SHA3-384, SHA3-512 Salt Length - 28, 32, 48, 64 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
RSA SigVer (FIPS186-5)	A7856, A7857, A7858, A7859, A7863, A7872, A7873	Hash Pair - Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Salt Length - 28, 32, 48, 64 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA-1	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
SHA2-224	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/256	A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA3-224	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-384	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHAKE-128	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Supports Bit-Oriented Messages - No Supports Empty Message - Yes Supports Bit-Oriented Output - No Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876	Supports Bit-Oriented Messages - No Supports Empty Message - Yes Supports Bit-Oriented Output - No Output Length - Output Length: 16-65536 Increment 8	FIPS 202

Table 5: Approved Algorithms

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric Cryptographic Key Generation (CKG)	Key Type:Asymmetric	N/A	SP 800-133r2, section 4, direct DRBG output without XOR

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 modes	Encryption, Decryption (not CAVP tested)
AES-GCM, CCM, GMAC, XTS keys not listed in the Security Function Implementations table of the Security Policy	Encryption, Decryption
AES using aes_*_generic function	Encryption, Decryption
AES GMAC using aes_*_generic	Message Authentication Generation
Curve secp256k1	Signature Generation, Signature Verification, Shared Secret Computation
Diffie Hellman	Shared Secret Computation (not CAVP tested)
HMAC-MD4, HMAC-MD5, HMAC-SHA1, HMAC-RIPEMD-160	Message Authentication Generation
MD4	Message Digest
MD5	Message Digest (outside of TLS)
RSA using RSA_generate_key_ex	Key Generation
ECDSA using EC_KEY_generate_key	Key Generation (not compliant with FIPS 186-5)
RSA using keys less than 2048 bits	Signature Generation
RSA using keys less than 1024 bits	Signature Verification
RSA	Key Encapsulation/Un-encapsulation, sign/verify

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Use and Function
	primitive operations without hashing
RSA with PKCS#1 v1.5 and OAEP padding	Encryption Primitive
SHA-1	Signature Generation
RIPEMD-160	Message Digest
TLS KDF using any SHA algorithms not listed in the Security Function Implementations table of the Security Policy or TLS KDF using non extended master secret	Key Derivation

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Key Generation with ML-DSA	AsymKeyPair-KeyGen CKG	FIPS 204. Key generation		ML-DSA KeyGen: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) Asymmetric Cryptographic Key Generation (CKG): ()
Signature Generation with ML-DSA	DigSig-SigGen	FIPS 204. Signature generation	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:pure Deterministic:No	ML-DSA SigGen: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Signature Generation with ML-DSA Internal	DigSig-SigGen	FIPS 204. Signature generation	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:internal	ML-DSA SigGen: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
			Deterministic:No External Mu:No	SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Signature Generation with ML-DSA External Mu	DigSig-SigGen	FIPS 204. Signature generation	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:internal Deterministic:No External Mu:Yes	ML-DSA SigGen: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Signature Verification with ML-DSA	DigSig-SigVer	FIPS 204. Signature verification	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:external Pre Hash:pure	ML-DSA SigVer: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Signature Verification with ML-DSA Internal	DigSig-SigVer	FIPS 204. Signature verification	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:internal External Mu:No	ML-DSA SigVer: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Signature Verification with ML-DSA External Mu	DigSig-SigVer	FIPS 204. Signature verification	Parameters:ML-DSA-44, ML-DSA-65, ML-DSA-87 Signature Interface:internal External Mu:Yes	ML-DSA SigVer: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Key Generation with ML-KEM	AsymKeyPair-KeyGen CKG	FIPS 203. Key generation	Parameters:ML-KEM-512, ML-KEM-768, ML-KEM-1024	ML-KEM KeyGen: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-512: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) Asymmetric Cryptographic Key Generation (CKG): ()
Key Encapsulation with ML-KEM	KEM-Encap	FIPS 203. Key encapsulation	Parameters:ML-KEM-512, ML-KEM-768, ML-KEM-1024 IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A7876) SHA3-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-512: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Key Decapsulation with ML-KEM	KEM-Decap	FIPS 203. Key decapsulation	Parameters:ML-KEM-512, ML-KEM-768, ML-KEM-1024 IG:IG D.S Scenario 1	ML-KEM EncapDecap: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-512: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Key Generation with ECDSA	AsymKeyPair-KeyGen CKG	FIPS 186-5. Key Generation		ECDSA KeyGen (FIPS186-5): (A7864) Asymmetric Cryptographic Key Generation (CKG): ()
Key Generation with EDDSA	AsymKeyPair-KeyGen CKG	FIPS 186-5. Key Generation		EDDSA KeyGen: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) Asymmetric Cryptographic Key Generation (CKG): ()
Key Generation with RSA	AsymKeyPair-KeyGen CKG	FIPS 186-5. Key Generation		RSA KeyGen (FIPS186-5): (A7864, A7873) Asymmetric Cryptographic Key Generation (CKG): ()

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
ECDSA Key Verification	AsymKeyPair-KeyVer	FIPS 186-5. Key Verification		ECDSA KeyVer (FIPS186-5): (A7855, A7856, A7857, A7858, A7859, A7863, A7864, A7871, A7872)
ECDSA Signature Generation	DigSig-SigGen	FIPS 186-5. Signature Generation		ECDSA SigGen (FIPS186-5): (A7855, A7856, A7857, A7858, A7859, A7862, A7863, A7865, A7871, A7872, A7874, A7875, A7876)
EDDSA Signature Generation	DigSig-SigGen	FIPS 186-5. Signature Generation		EDDSA SigGen: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
RSA Signature Generation	DigSig-SigGen	FIPS 186-5. Signature Generation		RSA SigGen (FIPS186-5): (A7855, A7856, A7857, A7858, A7859, A7862, A7863, A7865, A7871, A7872, A7873, A7874, A7875, A7876)
ECDSA Signature Verification	DigSig-SigVer	FIPS 186-5. Signature Verification		ECDSA SigVer (FIPS186-5): (A7855, A7856, A7857, A7858, A7859, A7862, A7863, A7865, A7871, A7872, A7874, A7875, A7876)
EDDSA Signature Verification	DigSig-SigVer	FIPS 186-5. Signature Verification		EDDSA SigVer: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
Legacy ECDSA Signature Verification	DigSig-SigVer	FIPS 186-4. Signature Verification		ECDSA SigVer (FIPS186-4): (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
Legacy RSA Signature Verification	DigSig-SigVer	FIPS 186-4. Signature Verification		RSA SigVer (FIPS186-4): (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872, A7873)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
RSA Signature Verification	DigSig-SigVer	FIPS 186-5. Signature Verification		RSA SigVer (FIPS186-5): (A7855, A7856, A7857, A7858, A7859, A7862, A7863, A7865, A7871, A7872, A7873, A7874, A7875, A7876)
Message Authentication Generation with AES	MAC	SP 800-38B, SP 800-38D. Message Authentication Generation		AES-CMAC: (A7839, A7844, A7849, A7860, A7866, A7869) AES-GMAC: (A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853, A7861, A7867, A7868, A7870)
Message Authentication Generation with HMAC	MAC	FIPS 198-1. Message Authentication Generation		HMAC-SHA-1: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-224: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-256: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-384: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-512: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-512/224: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA2-512/256: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) HMAC-SHA3-224:

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				(A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) HMAC-SHA3-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) HMAC-SHA3-384: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) HMAC-SHA3-512: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Message Authentication Verification with AES-GMAC	MAC	SP 800-38D. Message Authentication Verification		AES-GMAC: (A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853, A7861, A7867, A7868, A7870)
KAS-ECC-SSC Shared Secret Computation	KAS-SSC	SP 800-56Ar3. Shared Secret Computation	IG:IG D.F Scenario 2, path (1)	KAS-ECC-SSC Sp800-56Ar3: (A7864)
HKDF Key Derivation	KAS-56CKDF	SP 800-90Cr1. Key Derivation		KDA HKDF Sp800-56Cr1: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
SSH Key Derivation	KAS-135KDF	SP 800-135r1. Key Derivation		KDF SSH: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
TLS Key Derivation	KAS-135KDF	SP 800-135r1. Key Derivation		KDF TLS: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
PBKDF Key Derivation	PBKDF	SP 800-132. Key Derivation		PBKDF: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)
Message Digest	SHA XOF	FIPS 180-4, FIPS 202. Message Digest		SHA-1: (A7855, A7856, A7857, A7858, A7859,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A7863, A7871, A7872) SHA2-224: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA2-256: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA2-384: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA2-512: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA2-512/224: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA2-512/256: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872) SHA3-224: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-256: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-384: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHA3-512: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-128: (A7855, A7862, A7865, A7871, A7872, A7874, A7875, A7876) SHAKE-256: (A7855,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A7862, A7865, A7871, A7872, A7874, A7875, A7876)
Authenticated Encryption	BC-Auth	SP 800-38C, SP 800-38D, SP 800-38F. Authenticated Encryption		AES-CCM: (A7839, A7844, A7849, A7860, A7866, A7869) AES-GCM: (A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853, A7861, A7867, A7868, A7870) AES-KW: (A7839, A7844, A7849, A7860, A7866, A7869) AES-KWP: (A7839, A7844, A7849, A7860, A7866, A7869)
Authenticated Decryption	BC-Auth	SP 800-38C, SP 800-38D, SP 800-38F. Authenticated Decryption		AES-CCM: (A7839, A7844, A7849, A7860, A7866, A7869) AES-GCM: (A7840, A7841, A7842, A7843, A7845, A7846, A7847, A7848, A7850, A7851, A7852, A7853, A7861, A7867, A7868, A7870) AES-KW: (A7839, A7844, A7849, A7860, A7866, A7869) AES-KWP: (A7839, A7844, A7849, A7860, A7866, A7869)
Symmetric Encryption	BC-UnAuth	SP 800-38A, SP 800-38E. Encrypt a plaintext		AES-CBC: (A7839, A7844, A7849, A7860, A7866, A7869) AES-CTR: (A7839, A7844, A7849, A7860, A7866, A7869) AES-ECB: (A7839, A7840, A7841, A7842, A7843,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				A7844, A7845, A7846, A7847, A7848, A7849, A7850, A7851, A7852, A7853, A7860, A7861, A7866, A7867, A7868, A7869, A7870) AES-XTS Testing Revision 2.0: (A7839, A7844, A7849, A7854, A7860, A7866, A7869)
Symmetric Decryption	BC-UnAuth	SP 800-38A, SP 800-38E. Decrypt a ciphertext		AES-CBC: (A7839, A7844, A7849, A7860, A7866, A7869) AES-CTR: (A7839, A7844, A7849, A7860, A7866, A7869) AES-ECB: (A7839, A7840, A7841, A7842, A7843, A7844, A7845, A7846, A7847, A7848, A7849, A7850, A7851, A7852, A7853, A7860, A7861, A7866, A7867, A7868, A7869, A7870) AES-XTS Testing Revision 2.0: (A7839, A7844, A7849, A7854, A7860, A7866, A7869)
Random Number Generation	DRBG	SP 800-90Ar2. Random Number Generation		Counter DRBG: (A7839, A7844, A7849, A7860, A7866, A7869)
Key Derivation with KDA OneStep	KAS-56CKDF	SP 800-56Cr2. Key derivation		KDA OneStep SP800-56Cr2: (A7855, A7856, A7857, A7858, A7859, A7862, A7863, A7865, A7871, A7872, A7874, A7875, A7876)
Key Derivation with KBKDF	KBKDF	SP 800-108r1. Key derivation		KDF SP800-108: (A7855, A7856, A7857, A7858, A7859, A7863, A7871, A7872)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 the interfaces EVP_aead_aes_128_gcm_randnonce() and EVP_aead_aes_256_gcm_randnonce() for compliance with Scenario 2 of IG C.H and SP800-38D Section 8.2.2. The 96-bit AES-GCM IV, containing 96 bits of entropy, is generated randomly internal to the module using module's approved DRBG, without outputting the IV to the calling application. The DRBG is seeded from the entropy source.

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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

AES XTS

The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks, that is 16MB, of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E. The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit. To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical. Key_1 and Key_2 are generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

Key Derivation using SP 800-132 PBKDF2

The module provides password-based key derivation (PBKDF2), compliant with SP 800-132. The module supports option 1a from Section 5.4 of SP 800-132, in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK). In accordance 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**

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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, FIPS 186-4 RSA and ECDSA digital signature verification 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.

The use of SHA-1 for digital signature generation is non-approved. Starting January 1 of 2031 SHA-1 will be non-approved for all purposes.

Authenticated Encryption/Decryption

The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS. The authenticated algorithms are specified in the *Security Function Implementations* table.

KAS-SSC

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS. The algorithms offering KAS cryptographic functionality are specified in the *Security Function Implementations* table.

RSA Signature Generation and Signature Verification

The module provides RSA signature generation and signature verification compliant with IG C.F. The module supports RSA modulus lengths greater than or equal to 2048 bits for both signature generation and signature verification. The RSA signature generation and signature verification implementations have been tested for all module lengths available in CAVP testing: 2048, 3072, and 4096 bits. Legacy 186-4 signature verification is supported for the modulus size 1024. The RSA signature verification has been tested for all legacy module lengths available for CAVP testing: 1024 bits. The number of Miller-Rabin tests is consistent with the bit sizes of p and q from Table B.1 of FIPS 186-5.

SHA-3

SHA-3 is implemented as a standalone message digest algorithm and as part of the approved higher-level algorithms RSA SigGen/SigVer, ECDSA SigGen/SigVer, and KDA OneStep. Per IG C.C requirements, all SHA-3 functions and the higher-level algorithms that use SHA-3 have been tested and validated on all of the module's operating environments. The applicable CAVP certificates are listed in the *Approved Algorithms* table.

SHA-1

The SHA-1 algorithm is currently deprecated and will be non-approved for all purposes, starting January 1, 2031. The module doesn't offer signature generation or signature verification with SHA-1 in approved mode. Usage of SHA-

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 is in approved mode is only offered for Message Authentication Generation with HMAC, Message Digest, and Legacy RSA Signature Verification.

ML-KEM

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

[SP 800-227 RS6] ML-KEM SSPs are stored in RAM and the module provides methods to zeroize ML-KEM key pairs. If an application uses an ephemeral key pair, it is the obligation of the calling application to use the key pair for only one execution of key-establishment via a KEM and to destroy the key pair as soon as possible after its use.

[SP 800-227 RM3] When using an externally obtained ML-KEM static encapsulation key, the operator shall obtain assurance of possession of the corresponding decapsulation key prior to invoking the ML-KEM encapsulation service. Such assurance may be obtained through a trusted third party (e.g., a certificate authority) or another mechanism appropriate for the deployment, consistent with RM3 and Section 4.5 of SP 800-227.

[SP 800-227 RM4] All ML-KEM SSPs exist only in RAM for the duration of the service or handle, and are zeroized. The module shall not be operated in an operating environment that is using tools such as ptrace, gdb, strace, ftrace, systemtap, or userspace live patching. Physical and administrative security of the host is a deployment responsibility at Security Level 1.

[SP 800-227 RM5] The module does not perform key establishment and does not have a communications channel. Channel integrity is the responsibility of the calling application. The Approved Services table in Section 4.3 lists MAC and signature services the calling application can utilize to ensure channel security.

[SP 800-227 4.4] The module does not implement KEM key confirmation; where the application requires it, the calling application shall perform it using the module's approved MAC services.

ML-DSA

The module offers ML-DSA with both the external and internal signature interfaces. The module supports ML-DSA signature generation and verification using both the internal and external μ (Mu) interfaces. Per FIPS 204, the external μ shall be provided by another cryptographic module. Signature generation through the internal interface requires the calling application to construct the message representative M′. When the internal interfaces are used, the caller also supplies the 32-byte seed ξ consumed by ML-DSA.KeyGen_internal (FIPS 204, Algorithm 6) and the 32-byte rnd value consumed by ML-DSA.Sign_internal (Algorithm 7); these values shall be generated by an approved RBG, per FIPS 204 Section 3.5.

2.8 RBG and Entropy

Cert Number	Vendor Name
E280	Amazon

Table 10: Entropy Certificates

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
AWS-LC CPU Jitter RNG Entropy Source	Non-Physical	Amazon Linux 2023 on EC2 c6i.metal bare metal on Intel Ice Lake Xeon Platinum 8375C; Amazon Linux 2023 on EC2 c7a.metal bare metal on AMD Genoa AMD EPYC 4th Generation; Amazon Linux 2023 on EC2 r8g.metal-24xl bare metal on Amazon Graviton4 AWS Graviton	256	Full entropy	A7962 (SHA3-256)

Table 11: Entropy Sources

The module provides a 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 and reseeded with 384-bits of entropy. The entropy used for seeding and reseeding is provided from the SP800-90B compliant entropy source. This corresponds to scenario 1(b) of IG 9.3.A. Each call to the GetEntropy() interface returns at least 256 bits of entropy.

2.9 Key Generation

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

2.10 Key Establishment

The module offers ML-KEM Key Generation, Key Encapsulation and Key Decapsulation as independent approved services to the calling application. In the encapsulation service the operator supplies an ML-KEM encapsulation key and the module returns a shared secret key and the associated ciphertext; in the decapsulation service the operator supplies an ML-KEM decapsulation key and a ciphertext and the module returns the shared secret key. The shared secret key is output to the calling application, which is responsible for any subsequent use, and for performing the remaining steps of an approved KEM-based key-establishment scheme. Accordingly, no "KEM-Full" Security Function Implementation type is claimed.

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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API 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 12: 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 13: Roles

The module does not support concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
ML-KEM Key Generation	Generate a ML-KEM key pair	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Parameter Set, ML-KEM Seed (optional)	Module Generated ML-KEM Private Key, Module Generated ML-KEM Public Key	Key Generation with ML-KEM	Crypto Officer - Module Generated ML-KEM Public Key: G,R - Module Generated ML-KEM Private Key: G,R - ML-KEM Seed: W,E - Module Generated ML-KEM Seed: G,E - Intermediate Key Generation Value: G,E,Z

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
ML-KEM Key Encapsulation	Generate a shared secret key and the associated ciphertext using an ML-KEM encapsulation key	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	ML-KEM Public Key	ML-KEM Shared Secret Key, Ciphertext	Key Encapsulation with ML-KEM	Crypto Officer - ML-KEM Public Key: W,E - ML-KEM Shared Secret Key: G,R
ML-KEM Key Decapsulation	Recover the shared secret key from a ciphertext using an ML-KEM decapsulation key	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	ML-KEM Private Key, Ciphertext	ML-KEM Shared Secret Key	Key Decapsulation with ML-KEM	Crypto Officer - ML-KEM Private Key: W,E - ML-KEM Shared Secret Key: G,R
ML-DSA Key Generation	Generate a ML-DSA key pair	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Parameter Set, ML-DSA Seed (optional)	Module Generated ML-DSA Private Key, Module Generated ML-DSA Public Key	Key Generation with ML-DSA	Crypto Officer - Module Generated ML-DSA Public Key: G,R - Module Generated ML-DSA Private Key: G,R - ML-DSA Seed: W,E - Module Generated ML-DSA Seed: G,E - Intermediate Key Generation Value: G,E,Z

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
ML-DSA Signature Generation	Generate a digital signature with ML-DSA	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	ML-DSA private Key, message and context string (or ML-DSA message representative M′, or ML-DSA External Mu), ML-DSA Rnd (optional)	Digital Signature	Signature Generation with ML-DSA Signature Generation with ML-DSA Internal Signature Generation with ML-DSA External Mu	Crypto Officer - ML-DSA Private Key: W,E - ML-DSA External Mu: W,E - ML-DSA Rnd: W,E - Module Generated ML-DSA Rnd: G,E
ML-DSA Signature Verification	Verify a digital signature with ML-DSA	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	ML-DSA public key, signature, message and context string (or ML-DSA message representative M′, or ML-DSA External Mu)	Pass or Fail	Signature Verification with ML-DSA Signature Verification with ML-DSA Internal Signature Verification with ML-DSA External Mu	Crypto Officer - ML-DSA Public Key: W,E - ML-DSA External Mu: W,E
OneStep KDA Key Derivation	Derive a key from a shared secret	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Shared Secret	KDA OneStep Derived Key	Key Derivation with KDA OneStep	Crypto Officer - Shared Secret: W,E - ML-KEM Shared Secret Key: W,E - KDA OneStep Derived Key: G,R
Encryption	Encryption	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key, plaintext	Ciphertext	Symmetric Encryption	Crypto Officer - AES

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,E
Decryption	Decryption	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key, ciphertext	Plaintext	Symmetric Decryption	Crypto Officer - AES Key: W,E
Authenticated Encryption	Authenticated encryption	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key, IV, plaintext	Ciphertext, MAC tag	Authenticated Encryption	Crypto Officer - AES Key: W,E - GCM IV: W,E
Authenticated Decryption	Authenticated decryption	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key, ciphertext, MAC tag, IV	Plaintext	Authenticated Decryption	Crypto Officer - AES Key: W,E
Message Authentication Generation	MAC generation	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key/HMAC key, plaintext	MAC tag	Message Authentication Generation with AES Message Authentication Generation with HMAC	Crypto Officer - HMAC Key: W,E - AES Key: W,E
Message Authentication Verification	MAC verification	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	AES key, ciphertext, MAC tag, IV	Plaintext	Message Authentication Verification with AES-GMAC	Crypto Officer - AES Key: W,E
Message Digest	Generating message digest	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Message	Message digest	Message Digest	Crypto Officer
Random Number Generation	Generating random numbers	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Output length	Random bytes	Random Number Generation	Crypto Officer - Entropy Input (per IG D.L): W,E - DRBG Seed (per IG D.L): G,E

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State (V, Key) (per IG D.L): G,E
ECDSA Key Generation	Generating key pair	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Curve	Module Generated EC Private Key, Module Generated EC Public Key	Key Generation with ECDSA	Crypto Officer - Module generated EC Public Key: G,R - Module generated EC Private Key: G,R - Intermediate Key Generation Value: G,E,Z
RSA Key Generation	Generating key pair	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Modulus size	Module generated RSA public key, Module generated RSA private key	Key Generation with RSA	Crypto Officer - Module generated RSA Public Key: G,R - Module generated RSA Private Key: G,R - Intermediate Key Generation Value: G,E,Z
EDDSA Key Generation	Generating key pair	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Curve	Module Generated EC Private Key, Module Generated EC Public Key	Key Generation with EDDSA	Crypto Officer - Module generated EC Public Key: G,R - Module generated EC

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: G,R - Intermediate Key Generation Value: G,E,Z
Key Verification	Verifying the public key	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Public key	Success/ error	ECDSA Key Verification	Crypto Officer - EC Public Key: W,E
Signature Generation	Generating signature	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Message, EC private key or RSA private key	Digital signature	ECDSA Signature Generation RSA Signature Generation EDDSA Signature Generation	Crypto Officer - EC Private Key: W,E - RSA Private Key: W,E
Signature Verification	Verifying signature	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Signature, EC public key or RSA public key	Digital signature verification result	ECDSA Signature Verification Legacy ECDSA Signature Verification Legacy RSA Signature Verification RSA Signature Verification EDDSA Signature Verification	Crypto Officer - EC Public Key: W,E - RSA Public Key: W,E
Shared Secret Computation	Calculating the Shared Secret	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	EC public key, EC private key	Shared Secret	KAS-ECC-SSC Shared Secret	Crypto Officer - EC Public Key:

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Computation	W,E - EC Private Key: W,E - Shared Secret: G,R
TLS KDF Key Derivation	Deriving keys	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	TLS Pre-Master Secret, TLS Master Secret	TLS Master Secret, TLS Derived Key	TLS Key Derivation	Crypto Officer - TLS Pre-Master Secret: W,E - TLS Master Secret: G,E,R,Z - TLS Derived Key: G,R,Z
HKDF Key Derivation	Deriving keys	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Shared Secret	HKDF Derived key	HKDF Key Derivation	Crypto Officer - Shared Secret: W,E - ML-KEM Shared Secret Key: W,E - KDA HKDF derived key: G,R
SSH Key Derivation	Deriving keys	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Shared Secret	SSH KDF Derived Key	SSH Key Derivation	Crypto Officer - Shared Secret: W,E - ML-KEM Shared Secret Key: W,E - SSH KDF Derived Key: G,R

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PBKDF Key Derivation	Deriving keys	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Password	PBKDF Derived Key	PBKDF Key Derivation	Crypto Officer - Password: W,E - PBKDF Derived Key: G,R
KBKDF Key Derivation	Derive a key from a key-derivation key	Return value 1 from the function: CALL_SERVICE_AND_CHECK_APPROVED()	Key-Derivation Key	KBKDF Derived Key	Key Derivation with KBKDF	Crypto Officer - Key-Derivation Key: W,E - Shared Secret: W,E - ML-KEM Shared Secret Key: W,E - KBKDF Derived Key: G,R
Zeroization	Zeroize PSP in volatile memory	N/A	SSP	N/A	None	Crypto Officer - AES Key: Z - HMAC Key: Z - Entropy Input (per IG D.L): Z - DRBG Seed (per IG D.L): Z - DRBG Internal State (V, Key) (per IG D.L): Z - RSA Public Key: Z - RSA Private Key: Z - Module generated RSA

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key: Z - Module generated RSA Private Key: Z - EC Public Key: Z - EC Private Key: Z - Module generated EC Public Key: Z - Module generated EC Private Key: Z - Shared Secret: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Derived Key: Z - KDA HKDF derived key: Z - Password: Z - Intermediate Key Generation Value: Z - SSH KDF Derived Key: Z - PBKDF

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Derived Key: Z - ML-KEM Seed: Z - Module Generated ML-KEM Seed: Z - ML-DSA Seed: Z - Module Generated ML-DSA Seed: Z - ML-DSA Public Key: Z - ML-DSA Private Key: Z - ML-DSA External Mu: Z - ML-DSA Rnd: Z - Module Generated ML-DSA Rnd: Z - ML-KEM Public Key: Z - ML-KEM Private Key: Z - Module Generated ML-DSA Public Key: Z - Module Generated ML-DSA Private

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - Module Generated ML-KEM Public Key: Z - Module Generated ML-KEM Private Key: Z - ML-KEM Shared Secret Key: Z
On-Demand Self-test	Initiate power-on self-tests by reset	N/A	N/A	Pass or fail	Key Generation with ECDSA Key Generation with EDDSA Key Generation with ML-DSA Signature Generation with ML-DSA Signature Generation with ML-DSA Internal Signature Generation with ML-DSA External Mu Signature Verification with ML-DSA Signature Verification with ML-DSA Internal Signature Verificati	Crypto Officer

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					on with ML-DSA External Mu Key Generation with ML-KEM Key Encapsulation with ML-KEM Key Decapsulation with ML-KEM Key Generation with RSA ECDSA Key Verification ECDSA Signature Generation EDDSA Signature Generation RSA Signature Generation ECDSA Signature Verification EDDSA Signature Verification Legacy ECDSA Signature Verification Legacy RSA Signature Verification RSA	

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Signature Verification Message Authentication Generation with AES Message Authentication Generation with HMAC KAS-ECC-SSC Shared Secret Computation HKDF Key Derivation SSH Key Derivation TLS Key Derivation PBKDF Key Derivation Message Digest Authenticated Encryption Authenticated Decryption Symmetric Encryption Symmetric Decryption Random Number Generation	

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
On-Demand Integrity Test	Initiate integrity test on-demand	N/A	N/A	Pass or fail	None	Crypto Officer
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

Table 14: 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 function CALL_SERVICE_AND_CHECK_APPROVED(approved, func) invokes the service “func”, and either sets “approved” to a value of 1 indicating an approved service or a value of 0 indicating a non-approved service.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encryption	AES with OFB or CFB1, CFB8 modes AES-GCM, CCM, GMAC, XTS keys not listed in the Security Function Implementations table of the Security Policy AES using aes_*_generic function AES GMAC using aes_*_generic	CO
Decryption	Decryption	AES with OFB or CFB1, CFB8 modes AES-GCM, CCM, GMAC, XTS keys not listed in the Security Function Implementations table of the Security Policy 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-SHA1, HMAC-RIPEMD-160	CO

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Algorithms	Role
Message Digest	Generating message digest	MD4 MD5 RIPEMD-160	CO
Signature Generation	Generating signatures	RSA using keys less than 2048 bits RSA SHA-1	CO
Signature Verification	Verifying signatures	RSA using keys less than 1024 bits RSA	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 not listed in the Security Function Implementations table of the Security Policy or TLS KDF using non extended master secret	CO
Key Encapsulation	Encrypting a key	RSA with PKCS#1 v1.5 and OAEP padding	CO
Key Un-encapsulation	Decrypting a key	RSA with PKCS#1 v1.5 and OAEP padding	CO
Encryption Primitive	Asymmetric Encryption	RSA	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

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

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

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

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

8.1 Mitigation Techniques

The module claims no non-invasive security techniques.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 16: 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 17: 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
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded.	By calling the cipher related zeroization API
Automatic	Automatically zeroized by the module when no longer needed	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	N/A
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module

Table 18: SSP Zeroization Methods

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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	128-256 bits - 128-256 bits	Symmetric key - CSP			Message Authentication Generation with AES Message Authentication Verification with AES-GMAC Authenticated Encryption Symmetric Encryption Authenticated Decryption Symmetric Decryption
GCM IV	Initialization Vector for AES-GCM	96 bits - N/A	Initialization Vector - PSP			Message Authentication Generation with AES Message Authentication Verification with AES-GMAC Authenticated Encryption Authenticated Decryption
HMAC Key	HMAC Key	112-256 bits - 112-256 bits	Symmetric key - CSP			Message Authentication Generation with HMAC
Entropy Input (per IG D.L)	Entropy Input (per IG D.L)	256 bits - 256 bits	Entropy Input - CSP			Random Number Generation
DRBG Seed (per IG D.L)	DRBG Seed (per IG D.L)	256 bits - 256 bits	Seed - CSP	Random Number Generation		Random Number Generation
DRBG Internal State (V, Key) (per IG D.L)	DRBG Internal State (V, Key) (per IG D.L)	256 bits - 256 bits	Internal state - CSP	Random Number Generation		Random Number Generation
ML-KEM Seed	Seed used for Key	512 bits - 256 bits	Seed - CSP			Key Generation with ML-KEM

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Generation with ML-KEM					
ML-DSA Seed	Seed used for Key Generation with ML-DSA	256 bits - 256 bits	Seed - CSP			Key Generation with ML-DSA
ML-DSA Public Key	Used for signature verification	10496, 15616, 20736 bits - 128, 192, 256 bits	Public key - PSP			Signature Verification with ML-DSA Signature Verification with ML-DSA Internal Signature Verification with ML-DSA External Mu
ML-DSA Private Key	Used for signature generation	20480, 32256, 39168 bits - 128, 192, 256 bits	Private key - CSP			Signature Generation with ML-DSA Signature Generation with ML-DSA Internal Signature Generation with ML-DSA External Mu
ML-DSA External Mu	Externally computed ML-DSA message representative	512 bits - N/A	Message representative - PSP			Signature Generation with ML-DSA External Mu Signature Verification with ML-DSA External Mu
ML-DSA Rnd	Per-signature random value for Signature Generation with ML-DSA	256 bits - 256 bits	Random value - CSP			Signature Generation with ML-DSA Internal Signature Generation with ML-DSA External Mu
ML-KEM Public Key	Used for key encapsulation	6400, 9472, 12544 bits - 128, 192, 256 bits	Encapsulation key - PSP			Key Encapsulation with ML-KEM

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ML-KEM Private Key	Used for key decapsulation	13056, 19200, 25344 bits - 128, 192, 256 bits	Decapsulation key - CSP			Key Decapsulation with ML-KEM
Module Generated ML-DSA Seed	Seed used for Key Generation with ML-DSA	256 bits - 256 bits	Seed - CSP	Random Number Generation		Key Generation with ML-DSA
Module Generated ML-DSA Public Key	Used for signature verification	10496, 15616, 20736 bits - 128, 192, 256 bits	Public key - PSP	Key Generation with ML-DSA		
Module Generated ML-DSA Private Key	Used for signature generation	20480, 32256, 39168 bits - 128, 192, 256 bits	Private key - CSP	Key Generation with ML-DSA		
Module Generated ML-DSA Rnd	Per-signature random value for Signature Generation with ML-DSA	256 bits - 256 bits	Random value - CSP	Random Number Generation		Signature Generation with ML-DSA
Module Generated ML-KEM Seed	Seed used for Key Generation with ML-KEM	512 bits - 256 bits	Seed - CSP	Random Number Generation		Key Generation with ML-KEM
Module Generated ML-KEM Public Key	Used for key encapsulation	6400, 9472, 12544 bits - 128, 192, 256 bits	Encapsulation key - PSP	Key Generation with ML-KEM		
Module Generated ML-KEM Private Key	Used for key decapsulation	13056, 19200, 25344 bits - 128, 192, 256 bits	Decapsulation key - CSP	Key Generation with ML-KEM		
RSA Public Key	RSA Public Key	1024, 2048, 3072, 4096 bits -	Public key - PSP			Legacy RSA Signature Verification RSA

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		80-150 bits				Signature Verification
RSA Private Key	RSA Private Key	2048, 3072, 4096 bits - 112-150 bits of strength	Private key - CSP			RSA Signature Generation
Module generated RSA Public Key	Module generated RSA Public Key	2048, 3072, 4096 bits - 112-150 bits	Public key - PSP	Key Generation with RSA		
Module generated RSA Private Key	Module generated RSA Private Key	2048, 3072, 4096 bits - 112-150 bits	Private key - CSP	Key Generation with RSA		
Key-Derivation Key	Used for key derivation	112-4096 bits - 112-256 bits	Symmetric key - CSP			Key Derivation with KBKDF
KBKDF Derived Key	Generated by key-based key derivation	112-4096 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with KBKDF		
KDA OneStep Derived Key	Generated by OneStep KDA key derivation	2048 bits - 112-256 bits	Symmetric key - CSP	Key Derivation with KDA OneStep		
EC Public Key	EC Public Key	P-224, P-256, P-384, P-521, ED-25519 - 112-256 bits	Public key - PSP			ECDSA Key Verification ECDSA Signature Verification Legacy ECDSA Signature Verification KAS-ECC-SSC Shared Secret Computation
EC Private Key	EC Private Key	P-224, P-256, P-384, P-521,	Private key - CSP			ECDSA Signature Generation EDDSA

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		ED-25519 - 112-256 bits				Signature Generation KAS-ECC-SSC Shared Secret Computation
Module generated EC Public Key	Module generated EC Public Key	P-224, P-256, P-384, P-521, ED-25519 - 112-256 bits	Public key - PSP	Key Generation with ECDSA Key Generation with EDDSA		
Module generated EC Private Key	Module generated EC Private Key	P-224, P-256, P-384, P-521, ED-25519 - 112-256 bits	Private key - CSP	Key Generation with ECDSA Key Generation with EDDSA		
Shared Secret	Shared Secret	P-224, P-256, P-384, P-521 - 112-256 bits	Shared Secret - CSP		KAS-ECC-SSC Shared Secret Computation	HKDF Key Derivation SSH Key Derivation Key Derivation with KDA OneStep Key Derivation with KBKDF
TLS Pre-Master Secret	TLS Pre-Master Secret	P-224, P-256, P-384, P-521 - 112-256 bits	TLS pre-master secret - CSP			TLS Key Derivation
TLS Master Secret	TLS Master Secret	384 bits - 112-256 bits	TLS master secret - CSP	TLS Key Derivation		TLS Key Derivation
TLS Derived Key	Generated by TLS KDF key derivation	112-256 bits - 112-256 bits	Symmetric key - CSP	TLS Key Derivation		
KDA HKDF derived key	KDA HKDF derived key	112-2048 bits - 112-256 bits	Symmetric key - CSP	HKDF Key Derivation		

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH KDF Derived Key	SSH KDF Derived Key	112-256 bits - 112-256 bits	Symmetric key - CSP	SSH Key Derivation		
PBKDF Derived Key	PBKDF Derived Key	112-4096 bits - 112-256 bits of strength	Symmetric key - CSP	PBKDF Key Derivation		
Password	Password	112-1024 bits - N/A	Password - CSP			PBKDF Key Derivation
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 EDDSA Key Generation with ML-DSA Key Generation with ML-KEM		Key Generation with RSA Key Generation with ECDSA Key Generation with EDDSA Key Generation with ML-DSA Key Generation with ML-KEM
ML-KEM Shared Secret Key	Shared Secret Key generated by ML-KEM	256 bits - 128, 192, 256 bits	Shared Secret - CSP	Key Encapsulation with ML-KEM	Key Decapsulation with ML-KEM	HKDF Key Derivation SSH Key Derivation Key Derivation with KDA OneStep Key Derivation with KBKDF

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
GCM IV	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	AES Key:Used With
HMAC Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
Entropy Input (per IG D.L)	API input parameters	RAM:Plaintext	From service invocation to service completion	Automatic	DRBG Seed (per IG D.L):Generates
DRBG Seed (per IG D.L)		RAM:Plaintext	From service invocation to service completion	Automatic	Entropy Input (per IG D.L):Generated From DRBG Internal State (V, Key) (per IG D.L):Generates
DRBG Internal State (V, Key) (per IG D.L)		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	DRBG Seed (per IG D.L):Generated From
ML-KEM Seed	API input parameters	RAM:Plaintext	From service invocation to service completion	Automatic	Module Generated ML-KEM Private Key:Generates Module Generated ML-KEM Public Key:Generates
ML-DSA Seed	API input parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-DSA Private Key:Generates Module Generated ML-DSA Public Key:Generates
ML-DSA Public Key	API input parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	ML-DSA Private Key:Paired With ML-DSA External Mu:Verifies
ML-DSA Private Key	API input parameters	RAM:Plaintext	Until cipher handle is freed or	Wipe and Free memory	ML-DSA Public Key:Paired With

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			module is reset	block allocated Module Reset	ML-DSA External Mu:Signs
ML-DSA External Mu	API input parameters	RAM:Plaintext	From service invocation to service completion	Automatic	ML-DSA Private Key:Signed With ML-DSA Public Key:Verified With
ML-DSA Rnd	API input parameters	RAM:Plaintext	From service invocation to service completion	Automatic	ML-DSA Private Key:Signed With
ML-KEM Public Key	API input parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	ML-KEM Private Key:Paired With ML-KEM Shared Secret Key:Encapsulates
ML-KEM Private Key	API input parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	ML-KEM Public Key:Paired With ML-KEM Shared Secret Key:Decapsulates
Module Generated ML-DSA Seed		RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-DSA Private Key:Generates Module Generated ML-DSA Public Key:Generates
Module Generated ML-DSA Public Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-DSA Private Key:Paired With ML-DSA Seed:Derived From Module Generated ML-DSA Seed:Derived From Intermediate Key Generation Value:Generated From
Module Generated ML-DSA Private Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-DSA Public Key:Paired With ML-DSA Seed:Derived From Module Generated ML-DSA Seed:Derived From Intermediate Key

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Generation Value:Generated From
Module Generated ML-DSA Rnd		RAM:Plaintext	From service invocation to service completion	Automatic	ML-DSA Private Key:Signed With
Module Generated ML-KEM Seed		RAM:Plaintext	From service invocation to service completion	Automatic	Module Generated ML-KEM Private Key:Generates Module Generated ML-KEM Public Key:Generates
Module Generated ML-KEM Public Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-KEM Private Key:Paired With ML-KEM Seed:Derived From Module Generated ML-KEM Seed:Derived From Intermediate Key Generation Value:Generated From
Module Generated ML-KEM Private Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Module Generated ML-KEM Public Key:Paired With ML-KEM Seed:Derived From Module Generated ML-KEM Seed:Derived From Intermediate Key Generation Value:Generated From
RSA Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA Private Key:Paired With
RSA Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA Public Key:Paired With
Module generated	API output parameters	RAM:Plaintext	From service invocation to	Wipe and Free memory	Module generated RSA Private Key:Paired With

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RSA Public Key			service completion	block allocated Module Reset	Intermediate Key Generation Value:Generated From
Module generated RSA Private Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module generated RSA Public Key:Paired With Intermediate Key Generation Value:Generated From
Key-Derivation Key	API input parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	KBKDF Derived Key:Derives
KBKDF Derived Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Key-Derivation Key:Derived From
KDA OneStep Derived Key	API output parameters	RAM:Plaintext	Until cipher handle is freed or module is reset	Wipe and Free memory block allocated Module Reset	Shared Secret:Derived From
EC Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Private Key:Paired With Shared Secret:Generates
EC Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Public Key:Paired With Shared Secret:Generates
Module generated EC Public Key	API output parameters	RAM:Plaintext	From service invocation to service completion		Module generated EC Private Key:Paired With Intermediate Key Generation Value:Generated From

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Module generated EC Private Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Module generated EC Public Key:Paired With Intermediate Key Generation Value:Generated From
Shared Secret	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	EC Public Key:Derived From EC Private Key:Derived From
TLS Pre-Master Secret	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	TLS Master Secret:Derives
TLS Master Secret		RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	TLS Pre-Master Secret:Derived From TLS Derived Key:Derives
TLS Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	TLS Master Secret:Derived From
KDA HKDF derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Shared Secret:Derived From
SSH KDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	Shared Secret:Derived From
PBKDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	Password:Derived From

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Module Reset	
Password	API input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	PBKDF Derived Key:Derives
Intermediate Key Generation Value		RAM:Plaintext	From service invocation to service completion	Automatic	Module generated RSA Public Key:Generates Module generated RSA Private Key:Generates Module generated EC Public Key:Generates Module generated EC Private Key:Generates Module Generated ML-DSA Public Key:Generates Module Generated ML-KEM Private Key:Generates Module Generated ML-KEM Public Key:Generates Module Generated ML-DSA Private Key:Generates
ML-KEM Shared Secret Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	ML-KEM Public Key:Encapsulated by ML-KEM Private Key:Decapsulated by Module Generated ML-KEM Public Key:Encapsulated by Module Generated ML-KEM Private Key:Decapsulated by

Table 20: SSP Table 2

9.5 Transitions

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

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

FIPS 186-4 has been superseded by FIPS 186-5. FIPS 186-4 was withdrawn on February 3, 2024. The details regarding usage of Legacy algorithms are specified in Section 2.7.

Applying protection with keys with less than 128 bits of security will be non-approved for all algorithms starting January 1, 2031 as specified in SP 800-57 Part 1 Rev. 5, Section 5.6.3.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A7863)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7872)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7859)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7856)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7855)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7871)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7858)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o
HMAC-SHA2-256 (A7857)	SHA2-256	Message Authentication	SW/FW Integrity	Module becomes operational	Integrity test for bcm.o

Table 21: 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
SHA-1 (A7855)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7856)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7857)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7858)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A7859)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7863)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7871)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA-1 (A7872)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-256 (A7855)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7856)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7857)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7858)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7859)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7863)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7871)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-256 (A7872)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Module power-on before the integrity test
SHA2-512 (A7855)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7856)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7857)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7858)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7859)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A7863)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7871)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA2-512 (A7872)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7855)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7862)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7865)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7871)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7872)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7874)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7875)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
SHA3-256 (A7876)	SHA3-256	KAT	CAST	Module becomes operational	Message digest	Module power-on (not before integrity)
HMAC-SHA2-256 (A7855)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7856)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7857)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7858)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7859)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7863)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A7871)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
HMAC-SHA2-256 (A7872)	SHA-256	KAT	CAST	Module becomes operational	Message authentication	Module power-on before the integrity test
AES-CBC (A7839) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7844) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7849) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7860) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7866) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7869) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-CBC (A7839) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-CBC (A7844) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-CBC (A7849) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-CBC (A7860) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-CBC (A7866) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-CBC (A7869) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7840) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7841) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7842) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A7843) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7845) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7846) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7847) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7848) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7850) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7851) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7852) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7853) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7861) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7867) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7868) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7870) - Encrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric encryption	Module power-on (not before integrity)
AES-GCM (A7840) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7841) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7842) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7843) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A7845) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7846) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7847) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7848) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7850) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7851) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7852) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7853) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7861) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7867) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7868) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
AES-GCM (A7870) - Decrypt	128-bit keys	KAT	CAST	Module becomes operational	Symmetric decryption	Module power-on (not before integrity)
KDF SP800-108 (A7855)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7856)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7857)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7858)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SP800-108 (A7859)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7863)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7871)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDF SP800-108 (A7872)	Counter mode; HMAC-SHA-256; 256-bit input key	KAT	CAST	Module becomes operational	Key based key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7855)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7856)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7857)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7858)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7859)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7863)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7871)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA HKDF Sp800-56Cr1 (A7872)	SHA2-256; 256-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7855)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7856)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7857)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7858)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDA OneStep SP800-56Cr2 (A7859)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7862)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7863)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7865)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7871)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7872)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7874)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7875)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDA OneStep SP800-56Cr2 (A7876)	SHA2-256; 408-bit input secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Module power-on (not before integrity)
KDF TLS (A7855)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7856)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7857)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7858)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7859)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7863)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF TLS (A7871)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
KDF TLS (A7872)	SHA2-256	KAT	CAST	Module becomes operational	Industry-based TLS 1.0, 1.1 and 1.2 KDF key derivation	Module power-on (not before integrity)
PBKDF (A7855)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7856)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7857)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7858)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7859)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7863)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7871)	SHA-256; 18 character password; 288-bit salt; Iteration count: 2	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)
PBKDF (A7872)	SHA-256; 18 character password; 288-bit salt;	KAT	CAST	Module becomes operational	Password-based key derivation	Module power-on (not before integrity)

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	Iteration count: 2					
Counter DRBG (A7839)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
Counter DRBG (A7844)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
Counter DRBG (A7849)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
Counter DRBG (A7860)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
Counter DRBG (A7866)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
Counter DRBG (A7869)	AES-256	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 including health test per section 11.3	Module power-on (not before integrity)
KAS-ECC-SSC Sp800-56Ar3 (A7864)	P-256	KAT	CAST	Module becomes operational	Shared secret computation	First usage of key pair generation, signature generation, signature verification or shared secret computation services
RSA KeyGen (FIPS186-5) (A7864)	SHA-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-5) (A7873)	SHA-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA SigGen (FIPS186-5) (A7855)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification
RSA SigGen (FIPS186-5) (A7856)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7857)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7858)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7859)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7862)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7863)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7865)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7871)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature generation, signature verification
RSA SigGen (FIPS186-5) (A7872)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7873)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7874)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7875)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigGen (FIPS186-5) (A7876)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7855)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7856)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-5) (A7857)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7858)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7859)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7862)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7863)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7865)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7871)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7872)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification
RSA SigVer (FIPS186-5) (A7873)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7874)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7875)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
RSA SigVer (FIPS186-5) (A7876)	PKCS#1 v1.5 with SHA-256; 2048-bit key	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ML-KEM KeyGen KAT (A7855)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7862)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7865)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7871)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ML-KEM KeyGen KAT (A7872)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7874)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7875)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen KAT (A7876)	ML-KEM-512; KeyGen encapsulate; KeyGen decapsulate	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM KeyGen PCT	N/A	PCT	PCT	Successful key pair generation	Key encapsulation & decapsulation	Key pair generation
ML-KEM EncapDecap (A7855) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7862) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7865) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7871) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap	ML-KEM-512	KAT	CAST	Module becomes operational	Key encapsulation & decapsulation	First usage of key pair generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(A7872) - Encapsulate				and services are available for use		encapsulation or decapsulation services
ML-KEM EncapDecap (A7874) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7875) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7876) - Encapsulate	ML-KEM-512	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7855) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7862) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7865) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7871) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7872) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap	ML-KEM-512, implicit rejection path	KAT	CAST	Module becomes operational	Key encapsulation & decapsulation	First usage of key pair generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(A7874) - Decapsulate	and non-rejection path			and services are available for use		encapsulation or decapsulation services
ML-KEM EncapDecap (A7875) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-KEM EncapDecap (A7876) - Decapsulate	ML-KEM-512, implicit rejection path and non-rejection path	KAT	CAST	Module becomes operational and services are available for use	Key encapsulation & decapsulation	First usage of key pair generation, encapsulation or decapsulation services
ML-DSA KeyGen KAT (A7855)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7862)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7865)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7871)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7872)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7874)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services	Key generation	First usage of key pair generation, signature

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				are available for use		generation, signature verification
ML-DSA KeyGen KAT (A7875)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen KAT (A7876)	ML-DSA-44, Algorithm 6 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Key generation	First usage of key pair generation, signature generation, signature verification
ML-DSA KeyGen PCT	N/A	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ML-DSA SigGen (A7855)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7862)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7871)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7865)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7872)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification
ML-DSA SigGen (A7874)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7875)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigGen (A7876)	ML-DSA-44, Algorithm 7 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature generation	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7855)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7862)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7865)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7871)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7872)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational	Signature verification	First usage of key pair generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and services are available for use		signature generation, signature verification
ML-DSA SigVer (A7874)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7875)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
ML-DSA SigVer (A7876)	ML-DSA-44, Algorithm 8 FIPS 204	KAT	CAST	Module becomes operational and services are available for use	Signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA KeyGen (A7855)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7856)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7857)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7858)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7859)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7863)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7871)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA KeyGen (A7872)	ED-25519	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
EDDSA SigGen (A7855)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						generation, signature verification
EDDSA SigGen (A7856)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7857)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7858)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7859)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7863)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7871)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
EDDSA SigGen (A7872)	ED-25519	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
EDDSA SigVer (A7855)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7856)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7857)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7858)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7859)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7863)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7871)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
EDDSA SigVer (A7872)	ED-25519	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification
ECDSA KeyGen (FIPS186-5) (A7864)	SHA2-256	PCT	PCT	Successful key pair generation	SP800-56Ar3, 5.6.2.1.4, option (b)	Key pair generation
ECDSA SigGen (FIPS186-5) (A7855)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7856)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7857)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7858)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7859)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7862)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7863)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						signature verification
ECDSA SigGen (FIPS186-5) (A7865)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7871)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7872)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7874)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7875)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigGen (FIPS186-5) (A7876)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature generation	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7855)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation,

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-5) (A7856)						signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7857)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7858)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7859)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7862)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7863)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7865)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7871)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A7872)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7874)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7875)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification
ECDSA SigVer (FIPS186-5) (A7876)	SHA-256; P-256	KAT	CAST	Module becomes operational	Digital signature verification	First usage of key pair generation, signature generation, signature verification

Table 22: 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. Additionally, the module performs ML-KEM Decapsulation CASTs for both the implicit-rejection path and the non-rejection path.

Conditional Pair-Wise Consistency Tests

The module implements RSA, ECDSA, EDDSA, ML-DSA 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A7863)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7872)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7859)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7856)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7855)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7871)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7858)	Message Authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A7857)	Message Authentication	SW/FW Integrity	On demand	Manually

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A7855)	KAT	CAST	On Demand	Manually
SHA-1 (A7856)	KAT	CAST	On Demand	Manually
SHA-1 (A7857)	KAT	CAST	On Demand	Manually
SHA-1 (A7858)	KAT	CAST	On Demand	Manually
SHA-1 (A7859)	KAT	CAST	On Demand	Manually
SHA-1 (A7863)	KAT	CAST	On Demand	Manually
SHA-1 (A7871)	KAT	CAST	On Demand	Manually
SHA-1 (A7872)	KAT	CAST	On Demand	Manually
SHA2-256 (A7855)	KAT	CAST	On Demand	Manually
SHA2-256 (A7856)	KAT	CAST	On Demand	Manually
SHA2-256 (A7857)	KAT	CAST	On Demand	Manually
SHA2-256 (A7858)	KAT	CAST	On Demand	Manually
SHA2-256 (A7859)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A7863)	KAT	CAST	On Demand	Manually
SHA2-256 (A7871)	KAT	CAST	On Demand	Manually
SHA2-256 (A7872)	KAT	CAST	On Demand	Manually
SHA2-512 (A7855)	KAT	CAST	On Demand	Manually
SHA2-512 (A7856)	KAT	CAST	On Demand	Manually
SHA2-512 (A7857)	KAT	CAST	On Demand	Manually
SHA2-512 (A7858)	KAT	CAST	On Demand	Manually
SHA2-512 (A7859)	KAT	CAST	On Demand	Manually
SHA2-512 (A7863)	KAT	CAST	On Demand	Manually
SHA2-512 (A7871)	KAT	CAST	On Demand	Manually
SHA2-512 (A7872)	KAT	CAST	On Demand	Manually
SHA3-256 (A7855)	KAT	CAST	On Demand	Manually
SHA3-256 (A7862)	KAT	CAST	On Demand	Manually
SHA3-256 (A7865)	KAT	CAST	On Demand	Manually
SHA3-256 (A7871)	KAT	CAST	On Demand	Manually
SHA3-256 (A7872)	KAT	CAST	On Demand	Manually
SHA3-256 (A7874)	KAT	CAST	On Demand	Manually
SHA3-256 (A7875)	KAT	CAST	On Demand	Manually
SHA3-256 (A7876)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7855)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7856)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7857)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7858)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7859)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A7863)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7871)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7872)	KAT	CAST	On Demand	Manually
AES-CBC (A7839) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7844) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7849) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7860) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7866) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7869) - Encrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7839) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7844) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7849) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7860) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7866) - Decrypt	KAT	CAST	On Demand	Manually
AES-CBC (A7869) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7840) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7841) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7842) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7843) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7845) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7846) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7847) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7848) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7850) - Encrypt	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A7851) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7852) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7853) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7861) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7867) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7868) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7870) - Encrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7840) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7841) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7842) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7843) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7845) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7846) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7847) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7848) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7850) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7851) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7852) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7853) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7861) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7867) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7868) - Decrypt	KAT	CAST	On Demand	Manually
AES-GCM (A7870) - Decrypt	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7855)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF SP800-108 (A7856)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7857)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7858)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7859)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7863)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7871)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A7872)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7855)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7856)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7857)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7858)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7859)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7863)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7871)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A7872)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7855)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7856)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7857)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7858)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7859)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7862)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7863)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7865)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7871)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA OneStep SP800-56Cr2 (A7872)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7874)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7875)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A7876)	KAT	CAST	On Demand	Manually
KDF TLS (A7855)	KAT	CAST	On Demand	Manually
KDF TLS (A7856)	KAT	CAST	On Demand	Manually
KDF TLS (A7857)	KAT	CAST	On Demand	Manually
KDF TLS (A7858)	KAT	CAST	On Demand	Manually
KDF TLS (A7859)	KAT	CAST	On Demand	Manually
KDF TLS (A7863)	KAT	CAST	On Demand	Manually
KDF TLS (A7871)	KAT	CAST	On Demand	Manually
KDF TLS (A7872)	KAT	CAST	On Demand	Manually
PBKDF (A7855)	KAT	CAST	On Demand	Manually
PBKDF (A7856)	KAT	CAST	On Demand	Manually
PBKDF (A7857)	KAT	CAST	On Demand	Manually
PBKDF (A7858)	KAT	CAST	On Demand	Manually
PBKDF (A7859)	KAT	CAST	On Demand	Manually
PBKDF (A7863)	KAT	CAST	On Demand	Manually
PBKDF (A7871)	KAT	CAST	On Demand	Manually
PBKDF (A7872)	KAT	CAST	On Demand	Manually
Counter DRBG (A7839)	KAT	CAST	On Demand	Manually
Counter DRBG (A7844)	KAT	CAST	On Demand	Manually
Counter DRBG (A7849)	KAT	CAST	On Demand	Manually
Counter DRBG (A7860)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A7866)	KAT	CAST	On Demand	Manually
Counter DRBG (A7869)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A7864)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-5) (A7864)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-5) (A7873)	PCT	PCT	On Demand	Manually
RSA SigGen (FIPS186-5) (A7855)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7856)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7857)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7858)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7859)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7862)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7863)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7865)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7871)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7872)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7873)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7874)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7875)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7876)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7855)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7856)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7857)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7858)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7859)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A7862)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7863)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7865)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7871)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7872)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7873)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7874)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7875)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7876)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7855)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7862)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7865)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7871)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7872)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7874)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7875)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen KAT (A7876)	KAT	CAST	On Demand	Manually
ML-KEM KeyGen PCT	PCT	PCT	On Demand	Manually
ML-KEM EncapDecap (A7855) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7862) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7865) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7871) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7872) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7874) - Encapsulate	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ML-KEM EncapDecap (A7875) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7876) - Encapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7855) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7862) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7865) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7871) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7872) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7874) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7875) - Decapsulate	KAT	CAST	On Demand	Manually
ML-KEM EncapDecap (A7876) - Decapsulate	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7855)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7862)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7865)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7871)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7872)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7874)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7875)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen KAT (A7876)	KAT	CAST	On Demand	Manually
ML-DSA KeyGen PCT	PCT	PCT	On Demand	Manually
ML-DSA SigGen (A7855)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7862)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7871)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7865)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7872)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ML-DSA SigGen (A7874)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7875)	KAT	CAST	On Demand	Manually
ML-DSA SigGen (A7876)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7855)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7862)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7865)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7871)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7872)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7874)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7875)	KAT	CAST	On Demand	Manually
ML-DSA SigVer (A7876)	KAT	CAST	On Demand	Manually
EDDSA KeyGen (A7855)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7856)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7857)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7858)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7859)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7863)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7871)	PCT	PCT	On Demand	Manually
EDDSA KeyGen (A7872)	PCT	PCT	On Demand	Manually
EDDSA SigGen (A7855)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7856)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7857)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7858)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7859)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
EDDSA SigGen (A7863)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7871)	KAT	CAST	On Demand	Manually
EDDSA SigGen (A7872)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7855)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7856)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7857)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7858)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7859)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7863)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7871)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A7872)	KAT	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A7864)	PCT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7855)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7856)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7857)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7858)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7859)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7862)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7863)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7865)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7871)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7872)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7874)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A7875)	KAT	CAST	On Demand	Manually

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-5) (A7876)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7855)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7856)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7857)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7858)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7859)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7862)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7863)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7865)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7871)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7872)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7874)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7875)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7876)	KAT	CAST	On Demand	Manually

Table 24: 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	Pre-operational test failure: Error message is output (i.e., "FIPS integrity test failed.") on the stderr and then the module is aborted; Conditional test failure: For CAST failure, an error message indicating which KAT failed (e.g., "* KAT failed") is output on the stderr and then the module is aborted. Upon PCT failure, an error message indicating which PCT failed (e.g., "* keygen checks failed" or "* keygen PCT failed”) is output and the module is aborted. The abort statement indicates that the module is in error state.

Table 25: Error States

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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, ML-DSA 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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module bcm.o is embedded into the userspace 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/1276fc7d9cd0f509000294e9657914c3a23e65d2

The downloaded zip file can be verified by issuing the "sha256sum aws-lc-1276fc7d9cd0f509000294e9657914c3a23e65d2.zip" command. The expected SHA2-256 digest value is:

33b5443d2213bfca45071b300daeb45decf13e3b46f726890b48d6267968f049

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 three possible combinations of OS/processor, the module count is three (i.e., there are three separate binaries generated).

Amazon Linux 2023:

1. `sudo yum groupinstall "Development Tools"`
2. `sudo yum install cmake3 golang`
3. `cd aws-lc-fips-2025-09-12`
4. `mkdir build`
5. `cd build`
6. `cmake3 -DFIPS=1 -DCMAKE_BUILD_TYPE=RelWithDebInfo -DBUILD_SHARED_LIBS=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 4.0.0" 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 "dynamic" part can be done using following command with an application that was used for dynamic linking. The "U" in the output confirms that the module is dynamically linked.

Command: ***nm <application_name> | grep awslc_version_string***

Example Output: ***" U awslc_version_string"***

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

If the module is not installed following the instructions specified above, the "`./tool/bssl isfips`" command will output "0", the module will be in a non-compliant state and not considered a validated module in that state.

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.

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

11.3 Non-Administrator Guidance

N/A

**©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.**

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.

©2026 Amazon Web Services, Inc., atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.