



AWS-LC Cryptographic Module

Module Version: 2.0.0

FIPS 140-3 Non-Proprietary Security Policy

Document version: 1.0

Last update: 2023-10-25

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

1 Table of Contents

1	General.....	7
1.1	Overview.....	7
1.2	Security Levels	7
1.3	Additional Information	7
2	Cryptographic Module Specification	9
2.1	Description	9
2.2	Operating Environments.....	9
2.3	Excluded Components	10
2.4	Modes of Operation of the Module.....	10
2.5	Algorithms	10
2.6	Security Function Implementation	17
	Algorithm Specific Information	17
2.7	17	
2.7.1	GCM IV.....	17
2.7.2	AES XTS.....	18
2.7.3	Key Derivation using SP 800-132 PBKDF2	18
2.7.4	Compliance to SP 800-56ARev3 assurances	18
2.8	RNG and Entropy	19
2.9	Key Generation.....	19
2.10	Key Establishment	20
2.11	Industry Protocols.....	20
3	Cryptographic Module Interfaces	21
4	Roles, Services, and Authentication	22
4.1	Authentication Methods.....	22
4.2	Roles.....	22
4.3	Approved Services	22
4.4	Non-Approved Services.....	24
4.5	External Software/Firmware Loaded.....	24
5	Software/Firmware Security.....	25
5.1	Integrity Techniques	25
5.2	Initiate On-Demand Integrity Test	25
6	Operational Environment	26
6.1	Operational Environment Type and Requirements	26
	Configurable Settings and Restrictions.....	26
6.2	26	

7	Physical Security	27
8	Non-Invasive Security	28
9	Sensitive Security Parameter Management.....	29
9.1	Storage Areas	29
9.2	SSP Input-Output Methods.....	29
9.3	Zeroization Methods	29
9.4	SSPs.....	29
9.5	Transitions	32
10	Self-Tests	33
10.1	Pre-Operational Self-Test.....	33
10.2	Conditional Self-Tests	33
10.2.1	Conditional Cryptographic Algorithm Tests	35
10.2.2	Conditional Pair-Wise Consistency Tests	35
10.3	Periodic Self-Tests	35
10.4	Error States.....	35
10.5	Operator Initiation	35
11	Life-Cycle Assurance.....	36
11.1	Installation, Initialization and Startup Procedures.....	36
11.2	Administrator Guidance	37
12	Mitigation of Other Attacks.....	38
13	Glossary and Abbreviations	39
14	References.....	40

2 List of Tables

Table 1: Security Levels	7
Table 2: Tested Module Identification	9
Table 3: Tested Operational Environments	10
Table 4: Modes of Operation of the Module	10
Table 5: Approved Algorithms.....	16
Table 6: Vendor Affirmed Algorithms	16
Table 7: Non-Approved Allowed Algorithms with No Security Claimed	16
Table 8: Non-Approved Algorithms, Not Allowed in the Approved Mode of Operation	17
Table 9: Security Function Implementation.....	17
Table 10: Key Generation.....	19
Table 11: Key Establishment.....	20
Table 13: Ports and Interfaces	21
Table 14: Roles	22
Table 15: Approved Services.....	23
Table 16: Non-Approved Services	24
Table 17: Storage Areas.....	29
Table 18: SSP Input-Output.....	29
Table 19: Zeroization Methods.....	29
Table 20: SSP Information First.....	31
Table 21: SSP Information Second	32
Table 22: Pre-Operational Self-Tests.....	33
Table 23: Conditional Self-Tests.....	35
Table 24: Error States	35

3 List of Figures

Figure 1: Block diagram	9
-------------------------------	---

Copyrights and Trademarks

Amazon is a registered trademark of Amazon Web Services, Inc. or its affiliates.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 2.0.0 of the AWS-LC Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

1.2 Security Levels

Table 1 describes the individual security areas of FIPS 140-3, as well as the security levels of those individual areas.

ISO/IEC 24759 Section 6. Subsections	FIPS 140-3 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

Table 1: Security Levels

1.3 Additional Information

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

This 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.

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The AWS-LC Cryptographic Module (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

Module Characteristics: N/A

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 module components consist of the bcm.o file (version 2.0.0), which is statically linked to the userspace application during the compilation process.

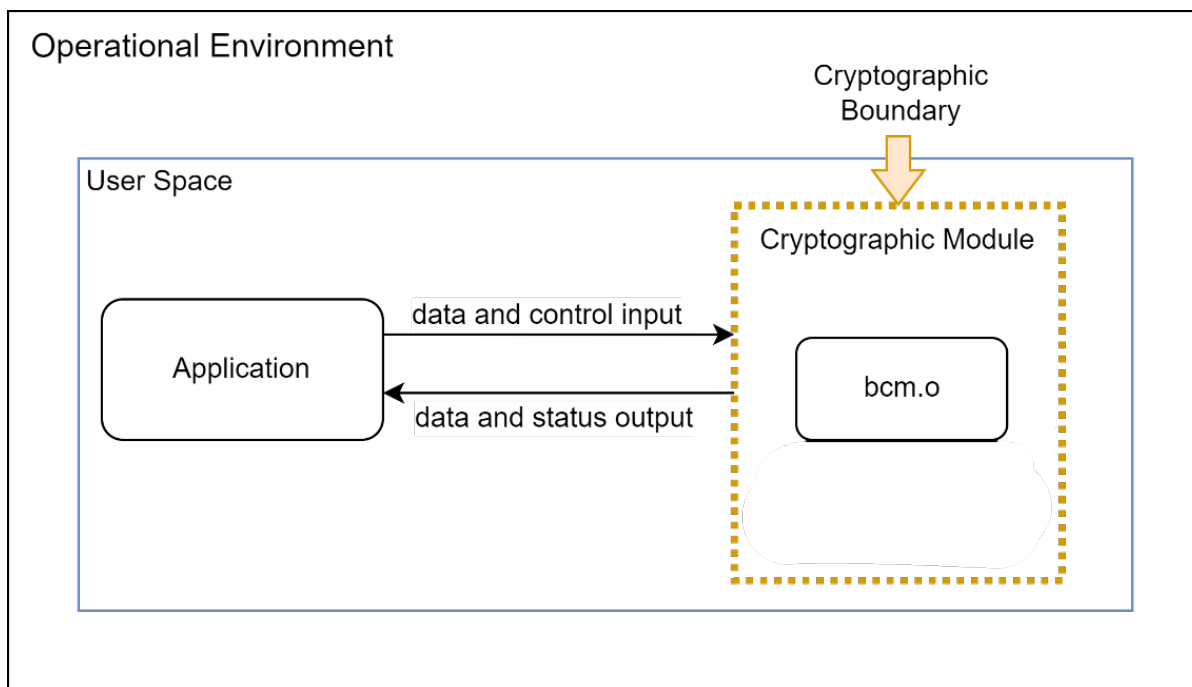


Figure 1: Block diagram

2.2 Operating Environments

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

Package/File Names	Software/ Firmware Version	Integrity Test Implemented
bcm.o	2.0.0	HMAC-SHA2-256

Table 2: Tested Module Identification

Tested Operational Environments - Software, Firmware, Hybrid:

© 2023 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	Processor(s)	PAA/PAI	Hypervisor or Host OS	Version(s)	
Amazon Linux 2	Amazon EC2 c5.metal with 192 GiB system memory and Elastic Block Store (EBS) 200 GiB	Intel ®Xeon ® Platinum 8275CL	AES-NI and SHA extensions (PAA)	N/A	2.0.0	
Amazon Linux 2023						
Ubuntu 22.04						
Amazon Linux 2	Amazon EC2 c6g.metal with 128 GiB system memory and Elastic Block Store (EBS) 200 GiB	Graviton3	Neon and Crypto Extension (CE) (PAA)		2.0.0	
Amazon Linux 2023						
Ubuntu 22.04						

Table 3: Tested Operational Environments

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation of the Module

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

Table 4: Modes of Operation of the Module

Mode change instructions and status indicators:

When the module starts up successfully, after passing the pre-operational self-test and the cryptographic algorithms self-tests (CASTs), the module is operating in the approved mode of operation by default and can only be transitioned into the non-approved mode by calling one of the non-approved services listed in Table 1516. Section 4 provides details on the service indicator implemented by the module. The service indicator identifies when an approved service is called.

Degraded Mode Description:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
AES-CBC	A4510, A4513, A4515, A4519, A4523, A4527	Encryption, Decryption	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, CE, VPAES Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, CE, VPAES Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, CE, VPAES Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM	FIPS197, SP800-38A, SP 800-38A Addendum
AES-CCM	A4510, A4513, A4515, A4519, A4523, A4527	Authenticated Encryption, Authenticated Decryption	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM	FIPS197, SP800-38C
AES- CMAC	A4510, A4513, A4515, A4519, A4523, A4527	Message Authentication Generation	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM	FIPS197, SP800-38B

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
AES-CTR	A4510, A4513, A4515, A4519, A4523, A4527	Encryption, Decryption	<p>Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES</p> <p>Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, BAES_CTASM, CE, VPAES</p> <p>Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES</p> <p>Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM</p> <p>Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM</p> <p>Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM</p>	FIPS 197, SP 800-38A, SP 800-38A Addendum
AES-ECB	A4510, A4511, A4512, A4513, A4514, A4515, A4516, A4519, A4520, A4521, A4522, A4523, A4524, A4525, A4526, A4527, A4528, A4529, A4530	Encryption, Decryption	<p>Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES, VPAES_GCM</p> <p>Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES, VPAES_GCM</p> <p>Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES, VPAES_GCM</p> <p>Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESNI_AVX, AESNI_ASM, AESASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM</p> <p>Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESNI_AVX, AESNI_ASM, AESASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM</p> <p>Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESNI_AVX, AESNI_ASM, AESASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM</p>	FIPS 197, SP 800-38A, SP 800-38A Addendum
AES-GCM	A4511, A4512, A4514, A4516, A4520, A4521, A4522, A4524, A4525, A4526,	Authenticated Encryption (with Internal IV Mode 8.2.2),		FIPS197, SP800-38D

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
AES-GCM	A4528, A4529, A4530	Authenticated Decryption (with external IV)	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES_GCM	FIPS197, SP800-38D
AES-GMAC		Message Authentication Generation	Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES_GCM Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, AES_C_GCM, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES_GCM Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: ASENI_AVX, AESNI_ASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: ASENI_AVX, AESNI_ASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: ASENI_AVX, AESNI_ASM, AESASM_AVX, AES_CLMULNI, AESASM_ASM, AESNI_CLMULNI, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM	FIPS197, SP800-38D
AES-KW	A4510, A4513, A4515, A4519, A4523, A4527	Key Wrapping, Key Unwrapping	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES	FIPS197, SP800-38F
AES-KWP				
AES-XTS		Encryption, Decryption	Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, AESNI, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, BAES_CTASM, CE, VPAES Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM	FIPS 197, SP 800-38E

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
CTR_DRBG	A4510, A4513, A4515, A4519, A4523, A4527	Random Number Generation	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: AES_C, CE, VPAES Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: AES_C, CE, VPAES Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: AES_C, CE, VPAES Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: AESNI, AESASM, BAES_CTASM	SP800-90Arev1
ECDSA	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Generation	Amazon Linux 2023 on EC2 bare metal on Amazon Graviton3: SHA_ASM, SHA_CE, NEON Ubuntu on EC2 bare metal on Amazon Graviton3 AWS Graviton: SHA_ASM, SHA_CE, NEON	FIPS 186-5 A.2.2 FIPS 186-5 Rejection Sampling
		Key Verification		FIPS 186-5
ECDSA with SHA2-224, SHA2-256, SHA2-384, SHA2-512		Signature Generation	Amazon Linux 2 on EC2 bare metal on Amazon Graviton3: SHA_ASM, SHA_CE, NEON Amazon Linux 2 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	
ECDSA with SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512		Signature Verification	Amazon Linux 2023 on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3 Ubuntu on EC2 bare metal on Intel Cascade Lake Xeon Platinum 8275CL: SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	
HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/256	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Message Authentication Generation		FIPS198-1
KAS-ECC-SSC ECC Ephemeral Unified scheme	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Shared Secret Computation		SP800-56ARev3

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
KDA HKDF with HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA2-512	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Derivation		SP800-56Crev1
KDF TLS 1.0/1.1/TLS 1.2 with SHA2-256, SHA2-384, SHA2-512	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Derivation		SP800-135rev1
PBKDF with HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Derivation (password based)		SP800-132 Option 1a
RSA	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Generation		FIPS 186-5 A.1.3 Random Probable Primes
RSA PKCS#1v1.5 with SHA2-224, SHA2-256, SHA2-384, SHA2-512 RSA PSS with SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256		Signature Generation		FIPS 186-5
RSA PKCS#1v1.5 with SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512; RSA PSS with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256		Signature Verification		
SSH KDF with AES-128, AES-192, AES-256; SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	A4509, A4517, A4518, A4531, A4532, A4533, A4534	Key Derivation		SP800-135rev1

Algorithm Name	CAVP Cert Numbers	Algorithm Capabilities	OE (Implementation)	Reference
SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/256	A4509, A4517, A4518, A4532, A4531, A4533, A4534	Message Digest		FIPS180-4

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Algorithm Name	Algorithm Capabilities	OE (Implementation)	References
Cryptographic Key Generation (CKG)	FIPS 186-5 Key generation RSA: 2048, 3072, 4096 bits with 112, 128, 149 bits of key strength. EC: P-224, P-256, P 384, P-521 elliptic curves with 112-256 bits of key strength	Software; OE same as in Table 3	SP 800-133Rev2 section 5.1 and 5.2

Table 6: Vendor Affirmed Algorithms

Non-Approved, Allowed Algorithms:

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:

Algorithm	Caveat	Use/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:

Algorithm/Functions	Use/Function
AES with OFB or CFB modes	Encryption, Decryption
AES GCM, GCM, GMAC, XTS with keys not listed in Table 5	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
HMAC-MD4, HMAC-MD5, HMAC-SHA1, HMAC-SHA-3	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
RSA using keys less than 2048 bits	Signature Generation
RSA using keys less than 1024 bits	Signature Verification

RSA	Key Wrapping, sign/verify primitive operations without hashing
RSA	Encryption primitive, PKCS#1 v1.5 and OAEP padding
SHA-1	Signature Generation
SHA-3	Message Digest
TLS KDF using any SHA algorithms not listed in Table 5	Key Derivation

Table 8: Non-Approved Algorithms, Not Allowed in the Approved Mode of Operation

2.6 Security Function Implementation

Name	Type	Description	SF Capabilities	Algorithms
KAS-ECC-SSC [SP 800-56ARev3]	KAS	Shared secret computation	Ephemeral Unified scheme Curves: P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of key strength Compliant with IG D.F scenario 2(1)	KAS-ECC-SSC: A4509, A4517, A4518, A4531, A4532, A4533, A4534
AES KW, AES-KWP [SP 800-38F]	KTS	Key wrapping, key unwrapping	128, 192, 256 bits with 128-256 bits of key strength Complaint with IG D.G	AES: A4510, A4513, A4515, A4519, A4523, A4527
AES GCM [SP 800-38D]	KTS	Key wrapping, key unwrapping	128, 256 bits with 128 and 256 bits of key strength Complaint with IG D.G	AES: A4511, A4512, A4514, A4516, A4520, A4521, A4522, A4524, A4525, A4526, A4528, A4529, A4530
AES CCM [SP 800-38C]	KTS	Key wrapping, key unwrapping	128 bits with 128 bits of key strength Complaint with IG D.G	AES: A4510, A4513, A4515, A4519, A4523, A4527

Table 9: Security Function Implementation

2.7 Algorithm Specific Information

2.7.1 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 via the functions `EVP_aead_aes_128_gcm_tls12()` and `EVP_aead_aes_256_gcm_tls12()`, 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 AES-GCM IV is generated randomly internal to the module using module's approved DRBG. The DRBG seeds itself from the entropy source. The GCM IV is 96 bits in length. Per Section 9, this 96-bit IV contains 96 bits of entropy.

Scenario 5, TLS 1.3

For TLS 1.3, the module offers the AES-GCM implementation via the functions `EVP_aead_aes_128_gcm_tls13()` and `EVP_aead_aes_256_gcm_tls13()`, and uses the context of Scenario 5 of IG C.H. The protocol that provides this compliance is TLS 1.3, defined in RFC8446 of 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.

2.7.2 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.

2.7.3 Key Derivation using SP 800-132 PBKDF2

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

2.7.4 Compliance to SP 800-56ARev3 assurances

The module offers ECDH shared secret computation services compliant to the SP 800-56ARev3 and meeting IG D.F scenario 2 path (1). To meet the required assurances listed in section 5.6 of SP

800-56Arev3, the module shall be used together with an application that implements the “TLS protocol” and the following steps shall be performed.

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

2.8 RNG and Entropy

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

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

2.9 Key Generation

Name	Type	Properties
ECDSA	CKG	EC: P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of key strength Method: FIPS 186-5 A.2.2 Rejection Sampling using a DRBG compliant with SP800-90Arev1 Compliant with SP800-133Rev2 section 5.1 and 5.2
RSA	CKG	RSA: 2048, 3072, 4096 bits with 112, 128, 149 bits of key strength. Method: FIPS 186-5 A.1.3 Random Probable Primes using a DRBG compliant with SP800-90Arev1 and SP800-133Rev2 section 5.1
KDA HKDF	Key Derivation	Key type: Symmetric key Security strength: 112-256 bits Method: SP 800-56Cr1; (HMAC) SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Compliant with SP800-133Rev2 section 6.2
PBKDF	Key Derivation	Key type: Symmetric key Security strength: 112-256 bits Method: option 1a of SP 800-132; (HMAC) SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Compliant with SP800-133Rev2 section 6.2
SSH	Key Derivation	Key type: Symmetric key Security strength: 112-256 bits Method: SP 800-135r1; AES-128, AES-192, AES-256 with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Compliant with SP800-133Rev2 section 6.2
TLS KDF	Key Derivation	Key type: Symmetric key Security strength: 112-256 bits Method: SP 800-135r1; SHA-256, SHA-384, SHA-512 Compliant with SP800-133Rev2 section 6.2

Table 10: Key Generation

2.10 Key Establishment

Name	Type	Properties
KAS-ECC-SSC [SP800-56Arev3]	KAS (Shared Secret Computation)	Curves: P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of key strength Compliant with IG D.F scenario 2(1)
AES GCM [SP 800-38D]	KTS-Wrap (Key wrapping, Key unwrapping)	128 and 256 bits with 128 and 256 bits of key strength Complaint with IG D.G
AES CCM [SP 800-38C]		128 bits with 128 bits of key strength Complaint with IG D.G
AES KW, AES KWP [SP 800-38F]		128, 192, 256 bits with 128-256 bits of key strength Complaint with IG D.G

Table 11: Key Establishment

2.11 Industry Protocols

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

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

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

3 Cryptographic Module Interfaces

As a Software module, the module interfaces are defined as Software or Firmware Module Interfaces (SMFI), and there are no physical ports.

Logical Interface	Data that passes over port/interface
Data Input	API input parameters for data.
Data Output	API output parameters for data.
Control Input	API function calls.
Status Output	API return codes, error message.

Table 12: Ports and Interfaces²

² The control output interface is omitted on purpose because the module does not implement it. The physical ports are not applicable because the module is software only.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication.

4.2 Roles

The module does not support concurrent operators.

Name	Type	Operator Type	Authentication
Crypto Officer	Role	CO	N/A (Implicitly assumed)

Table 13: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
Encryption	Encryption	Return value 1 from the function: FIPS_service_indicator_check_approved()	AES key, plaintext	Ciphertext	AES CBC, CTR, ECB, XTS	CO	AES Key: W, E
Decryption	Decryption		AES key, ciphertext	Plaintext	listed in Table 5		
Authenticated Encryption	Authenticated Encryption		AES key, plaintext	Ciphertext	AES CCM AES GCM listed in Table 5		AES Key: W, E
Authenticated Decryption	Authenticated Decryption		AES key, ciphertext	Plaintext			
Key wrapping	Encrypting a key		AES key wrapping key, Key to be wrapped	Wrapped key	AES KW, KWP, CCM, GCM		AES key: W, E
Key unwrapping	Decrypting a key		AES key unwrapping key	Unwrapped key	AES KW, KWP, CCM, GCM		AES key: W, E
Message Authentication Generation	MAC computation		AES key, message	MAC tag	AES CMAC, GMAC		AES Key: W, E
			HMAC key, message		HMAC		HMAC Key: W, E
Message Digest	Generating message digest		Message	Message digest	SHA		N/A
Random Number Generation	Generating random numbers		Output length	Random bytes	CTR_DRBG		Entropy Input: W, E
							DRBG Seed, V, Key: G, E
Key Generation	Generating key pair		Modulus size	RSA public key, RSA private key	RSA listed in Table 5 CKG		RSA Public Key: G, R; RSA Private Key: G, R
		Curve	EC public key, EC private key	ECDSA listed in Table 5, CKG	EC Public Key: G, R; EC Private Key: G, R		
Key Verification	Verifying the public key		Public key	Success/error	ECDSA listed in Table 5	ECDSA Public Key: W, E	

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
Signature Generation	Generating signature		Message, EC private key or RSA private key	Digital signature	RSA, ECDSA listed in Table 5		RSA/ECDSA Private Key: W, E
Signature Verification	Verifying signature		Signature, EC public key or RSA public key	Digital signature verification result	RSA, ECDSA listed in Table 5		RSA/ECDSA Public Key: W, E
Shared Secret Computation	Calculating the Shared Secret		EC public key, EC private key	Shared Secret	KAS-ECC-SSC		EC Public Key: W, E; EC Private Key: W, E
							Shared Secret: G, R
Key Derivation	Deriving Keys		TLS Pre-Master Secret	TLS Master secret	TLS KDF 1.0/1.1/1.2, KDA HKDF		TLS Pre-Master Secret: W, E
			TLS Master Secret	Derived Key	TLS KDF 1.0/1.1/1.2, KDA HKDF		TLS Master Secret: W, E, G; TLS Derived Keys: G; Derived Key: G, R
			Password, salt, iteration count		PBKDF2		Derived Key: G, R; Password: W, E
			Shared Secret, Key Length, Digest		KDA HKDF		Derived Key: G, R; Shared Secret: W, E
		Shared Secret, Key Length	SSH KDF		Derived Key: G, R		
Zeroization	Zeroize PSP in volatile memory	N/A	SSP	N/A	None	All SSPs: Z	
On-Demand Self-test	Initiate power-on self-tests by reset		N/A	Pass or fail	AES, HMAC, SHA, DRBG, RSA, ECDSA, KAS ECC SSC, TLS KDF, KDA HKDF, PBKDF	N/A	
On-Demand Integrity Test	Initiate integrity test on-demand		N/A		HMAC-SHA2-256	N/A	
Show Status	Show status of the module state		N/A	Module status	N/A	N/A	
Show Version	Show the version of the module using awslc_version_string		N/A	Module name and version	N/A	N/A	

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.

- G = Generate: The module generates or derives the SSP.

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

For the role, CO indicates “Crypto Officer”.

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

- STEP 1: Should be called before invoking the service.
`int before = FIPS_service_indicator_before_call();`
- STEP 2: Make a service call i.e., API function for performing a service.
`Func();`
- STEP 3: Should be called after invoking the service.
`int after = FIPS_service_indicator_after_call();`
- STEP 4: Return value 1 indicates approved service was invoked.
`int ret = FIPS_service_indicator_check_approved(before, after);`

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

4.4 Non-Approved Services

Service	Description	Algorithms Accessed	Role	Indicator
Encryption	Encryption	AES listed in Table 8	CO	Return value 0 from the function <code>FIPS_service_indicator_check_approved()</code>
Decryption	Decryption			
Message Authentication Generation	MAC computation	AES GMAC and HMAC listed in Table 8		
Message Digest	Generating message digest	MD4, MD5 outside TLS 1.0 usage, SHA-3		
Signature Generation	Generating signature	Using SHA-1		
		RSA listed in Table 8, Curve secp256k1		
Signature Verification	Verifying signature	RSA listed in Table 8, Curve secp256k1		
Key Generation	Generating key pair	RSA or ECDSA listed in Table 8		
Shared Secret Computation	Calculating shared secret	Diffie-Hellman, Curve secp256k1		
Key Derivation	Deriving TLS keys	TLS KDF listed in Table 8		
Key Encapsulation	Decrypting a key	RSA		
Key Un-encapsulation	Encrypting a key	RSA		

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

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

5 Software/Firmware Security

5.1 Integrity Techniques

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

5.2 Initiate On-Demand Integrity Test

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: The module operates in a modifiable operational environment. The module runs on a commercially available general-purpose operating system executing on the hardware specified in section 2.

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 Configurable 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 `fttrace` or `systemtap`, shall not be used in the operational environment. The use of any of these tools implies that the cryptographic module is running in a non-validated operational environment.

7 Physical Security

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

8 Non-Invasive Security

The module claims no non-invasive security techniques.

9 Sensitive Security Parameter Management

9.1 Storage Areas

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

Table 16: Storage Areas

9.2 SSP Input-Output Methods

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

Table 17: SSP Input-Output

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 Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Free Cipher Handle	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	By calling the appropriate zeroization functions: <code>OpenSSL_cleanse,</code> <code>EVP_CIPHER_CTX_cleanup,</code> <code>EVP_AEAD_CTX_zero,</code> <code>HMAC_CTX_cleanup,</code> <code>CTR_DRBG_clear,</code> <code>RSA_free,</code> <code>EC_KEY_free</code>
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: Zeroization Methods

9.4 SSPs

Name	Description	Size	Strength	Type	Generation	Established By
AES Key	AES key used for encryption, decryption, and computing MAC tags	128-256 bits	128-256 bits of strength	Symmetric key	N/A	N/A
HMAC Key	HMAC key for Message	112-524288	112-256 bits of	Authentication	N/A	N/A

Name	Description	Size	Strength	Type	Generation	Established By
	Authentication Generation	bits	strength	key		
Entropy Input	Entropy input used to seed the DRBGs	256 bits	256 bits of strength	Entropy	N/A	N/A
DRBG Seed	DRBG seed derived from entropy input as defined in SP 800-90Ar1	256 bits	256 bits of strength	DRBG seed	CTR_DRBG (according to SP800-90Arev1)	N/A
DRBG Internal State (V, Key)	Internal state of CTR_DRBG	256 bits	256 bits of strength	Internal state	CTR_DRBG (derived from DRBG seed according to SP800-90Ar1)	N/A
RSA Public Key	RSA public key used for RSA key generation, signature verification	1024, 2048, 3072, 4096 bits	80-150 bits of strength	Public key	RSA (generated according to FIPS 186-5) DRBG (for generation of random values)	N/A
RSA Private Key	RSA private key used for RSA key generation, signature generation			Private key		N/A
EC Public Key	EC public key used for EC key generation, key verification, signature verification, shared secret computation	P-224, P-256, P-384, P-521	112-256 bits of strength	Public key	ECDSA (generated according to FIPS 186-5) DRBG (for generation of random values)	N/A
EC Private Key	EC private key used for EC key generation, key verification, signature generation, shared secret computation			Private key		N/A
Shared Secret	Shared Secret generated by KAS-ECC-SSC			Shard secret	N/A	KAS-ECC-SSC (established according to SP800-56Arev3)
TLS Pre-Master Secret	TLS Pre-Master secret used for deriving the TLS Master Secret	112-256 bits	N/A	TLS pre-master secret	N/A	KAS-ECC-SSC (established according to SP800-56Arev3)
TLS Master Secret	TLS Master secret used for deriving the TLS Derived Key	384 bits	N/A	TLS Master secret	TLS KDF (derived according to SP800-135rev1)	N/A
TLS Derived key (AES/HMAC)	TLS Derived Key from TLS Master Secret	AES: 128-256 bits HMAC: 112 to 256 bits	AES: 128-256 bits of strength HMAC: 112-256 bits of strength	Symmetric key		N/A
Derived Key	KDA HKDF derived	112 to 256 bits	N/A	Symmetric key	KDA HKDF (derived)	N/A

Name	Description	Size	Strength	Type	Generation	Established By
	key				according to SP800-56Crev1)	
	SSH KDF derived key				SSH KDF (derived according to SP800-135rev1)	
	PBKDF derived key				PBKDF (derived according to SP800-132)	
Password	Password for PBKDF	0-256 bits	N/A	Password	N/A	N/A
Intermediate Key Generation Value	Intermediate key generation value	224-4096	112-256 bits of strength	Intermediate value	CKG	N/A

Table 19: SSP Information First

Name	Used By	Inputs/Outputs	Storage	Zeroization	Category	Related SSPs
AES Key	Encryption, Decryption, Authenticated Encryption, Authentication Decryption, Key wrapping, Key unwrapping, Message Authentication Generation	API input parameters (input)	RAM	Free Cipher Handle, Module Reset	CSP	None
HMAC Key	Message Authentication Generation	API input parameters (input)			CSP	None
Entropy Input	Random Number Generation	N/A		Automatically	CSP	DRBG Seed
DRBG Seed	Random Number Generation	N/A			CSP	Entropy Input, DRBG Internal State
DRBG Internal State (V, Key)	Random Number Generation	N/A		Free Cipher Handle, Module Reset	CSP	DRBG Seed
RSA Public Key	Key Generation, Signature Verification	API input parameters (input), API output parameters (output)			PSP	RSA Private Key
RSA Private Key	Key Generation, Signature Generation	API output parameters (output)			CSP	RSA Public Key
EC Public Key	Key Generation, Key Verification, Signature Verification, Shared Secret Computation	API input parameters (input), API output parameters (output)			PSP	EC Private Key, Shared Secret

Name	Used By	Inputs/Outputs	Storage	Zeroization	Category	Related SSPs
EC Private Key	Key Generation, Key Verification, Signature Generation, Shared Secret Computation				CSP	EC Public Key, Shared Secret
Shared Secret	Shared Secret Computation	API output parameters (output)			CSP	EC Public Key,
TLS Pre-Master Secret	Key Derivation	N/A			CSP	TLS Master Secret
TLS Master Secret	Key Derivation	N/A			CSP	TLS Pre-Master Secret
TLS Derived Key (AES/HMAC)	Key Derivation	API output parameters (output)			CSP	TLS Master Secret
Derived Key		API output parameters (output)			CSP	Key Derivation Key, Shared Secret, Password
Key Derivation Key		API input parameters (input)			CSP	Derived Key
Password					CSP	
Intermediate Key Generation Value	Key generation	N/A		Automatically	CSP	RSA Private Key, RSA Public Key, EC Private Key, EC Public Key

Table 20: SSP Information Second

9.5 Transitions

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

10 Self-Tests

10.1 Pre-Operational Self-Test

Algorithm	Implementation	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256	SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	SHA2-256	Message Authentication	Software Integrity	Module becomes operational	N/A

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 includes the self-test for HMAC-SHA2-256 algorithm used in the pre-operational self-test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Condition	Coverage	Coverage Notes
AES CBC AES GCM AES_C, AES_C_GCM, AESNI, AESNI_AVX, AESNI_ASM, AESAESM, AESASM_AVX, AESASM_CLMULNI, AESASM_ASM, CE, CE_GCM_UNROLL8_EOR3, CE_GCM, VPAES, VPAES_GCM, AESNI_CLMULNI, BAES_CTASM, BAES_CTASM_AVX, BAES_CTASM_CLMULNI, BAES_CTASM_ASM	128-bit AES key	Encrypt KAT for CBC	CAST	Module is operational	Encrypt	Power up	Self	N/A
		Decrypt KAT for CBC			Decrypt		Self and ECB, KW, KWP, XTS (all implementations)	IG 10.3.A, resolution 1.c
		Encrypt KAT for GCM			Encrypt		Self and CCM, CMAC, CTR, ECB, GMAC, KW, KWP, XTS all implementations)	IG 10.3.A, resolution 1.d.(i)
		Decrypt KAT for GCM			Decrypt		Self	N/A
SHA-1 SHA-256 SHA_CE, SHA_ASM, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	N/A	SHA-1 KAT	CAST	Message digest	Power up	Power up	Self	N/A
		SHA2-256 KAT					SHA-224 all implementations)	IG 10.3.A, resolution 2
		SHA2-512 KAT					SSH (all implementations)	IG 10.3.A, resolution 12, note 18
							SHA2-384, SHA2-512/256 (all implementations)	IG 10.3.A, resolution 2
CTR_DRBG AES_C, AESNI, AESASM, AESASM_AVX,	AES 256	CTR_DRBG KAT	CAST		Seed Generation	Power up	Self	N/A

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Condition	Coverage	Coverage Notes
CE, VPAES, BAES_CTASM	N/A	SP800-90Ar1 Section 11.3 Health Test			Seed Generation	Power up	Self	N/A
ECDSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	P-256 Curve and SHA2-256	Sign KAT	CAST		Sign	Signature Generation or Key Generation service request	Self	N/A
ECDSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	P-256 Curve and SHA2-256	Verify KAT			Verify	Signature verification or Key Generation service request	Self	N/A
KAS-ECC-SSC C	P-256 Curve	Z computation			Shared secret computation	Shared secret computation request	Self	N/A
ECDSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	Respective Curve and SHA2-256	Signature generation and verification	PCT		Sign and Verify	Key generation	Self and KAS-ECC-SSC PCT	IG 10.3.A additional comment 1.
TLS KDF SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	SHA2-256	TLS 1.2 KAT	CAST		Key derivation	Power up	Self	N/A
KDA HKDF SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	HMAC-SHA2-256	KAT	CAST		Key derivation	Power up	Self	N/A
PBKDF2 SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	HMAC-SHA2-256	KAT	CAST		Key derivation	Power up	Self and HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/256	IG 10.3.A resolution 5 and IG 10.3.B
RSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	PKCS#1 v1.5 with 2048 bit key and SHA2-256	Sign KAT	CAST		Sign	Signature Generation or Key Generation service request	Self	N/A
RSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	PKCS#1 v1.5 with 2048 bit key and SHA2-256	Verify KAT	CAST		Verify	Signature Verification or Key Generation service request	Self	N/A

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Condition	Coverage	Coverage Notes
RSA SHA_ASM, SHA_CE, NEON, SHA_SHANI, SHA_AVX2, SHA_AVX, SHA_SSSE3	SHA2-256 and respective keys	Signature generation and verification	PCT		Sign and Verify	Key generation	Self	N/A

Table 22: Conditional Self-Tests

10.2.1 Conditional Cryptographic Algorithm Tests

The module performs self-tests on approved cryptographic algorithms, using the tests shown in Table 2223. 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.

10.2.2 Conditional Pair-Wise Consistency Tests

The module implements RSA and ECDSA key generation service and performs the respective pairwise consistency test (PCT) using sign and verify functions when the keys are generated (Table 2223). If any of these self-tests fails, the module transitions to error state and is aborted.

10.3 Periodic Self-Tests

The module does not support periodic self-tests.

10.4 Error States

Name	Description	Condition	Recovery Method	Status Indicator
Error	The library is aborted with SIGABRT signal. Module is no longer operational the data output interface is inhibited	Pre-operational test failure	Module reset	Error message is output on the stderr and then the module is aborted.
		Conditional test failure	Module reset	Error message is output in the error queue and then the module generates new key, If the PCT still does not pass, eventually the module will be aborted after 5 tries.

Table 23: Error States

If the module fails any of the self-tests, the module enters the error state. To recover from the Error state, the module needs to be rebooted.

10.5 Operator Initiation

The software integrity tests and the CASTs for AES, SHS, DRBG, KAS-ECC-SSC, TLS KDF, KDA HKDF, PBKDF2 can be invoked by unloading and subsequently re-initializing the module. The CASTs for ECDSA and RSA can be invoked by requesting the corresponding Key Generation or Digital Signature services. Additionally, all the CASTs can be invoked by calling the BORINGSSL_self_test function. The PCTs can be invoked on demand by requesting the Key Generation service.

11 Life-Cycle Assurance

11.1 Installation, Initialization and Startup Procedures

The module `bcm.o` is embedded into the 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/archive/refs/heads/fips-2022-11-02.zip>

The downloaded zip file can be verified by issuing the “`sha256sum aws-lc-fips-2022-11-02.zip`” command. The expected SHA2-256 digest value is:
`5b319882e70cf8f692c983a7291d6329773cae24290fe4c9b1a2640dcd64bfe8`

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 four possible combinations of OS/processor, the module count is six (i.e., there are six separate binaries generated, one for each entry listed in Table 3).

Amazon Linux 2 and Amazon Linux 2023:

1. `sudo yum groupinstall "Development Tools"`
2. `sudo yum install cmake3 golang`
3. `cd ~/aws-lc-fips-2022-11-02/`
4. `mkdir build`
5. `cd build`
6. `cmake3 -DFIPS=1 ..`
7. `make`

Ubuntu 22.04:

1. `sudo apt-get install build-essential`
2. `sudo apt-get install cmake`
3. Get latest Golang archive for your architecture,
e.g., `wget https://go.dev/dl/go1.20.5.linux-amd64.tar.gz` or
`wget https://go.dev/dl/go1.20.5.linux-arm64.tar.gz`
4. `sudo tar -C /usr/local -xzf go*.tar.gz`
5. `cd ~/aws-lc-fips-2022-11-02/`
6. `mkdir build`
7. `cd build`
8. `cmake -DFIPS=1 -DGO_EXECUTABLE=/usr/local/go/bin/go ..`
9. `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 in 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 2.0.0” which is the module version. Additionally, the “AWS-LC FIPS” also acts as the module identifier. This will confirm that the module is in the operational mode.

11.2 Administrator Guidance

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 and provide a new replacement.

12 Mitigation of Other Attacks

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.

13 Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
CAVP	Cryptographic Algorithm Validation Program
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMT	Cryptographic Module Testing
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards Publication
FSM	Finite State Model
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
KW	AES Key Wrap
KWP	AES Key Wrap with Padding
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OFB	Output Feedback
O/S	Operating System
PAA	Processor Algorithm Acceleration
PCT	Pair-Wise Consistency Test
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

14 References

- FIPS140-3** **FIPS PUB 140-3 - Security Requirements for Cryptographic Modules**
March 2019
<https://doi.org/10.6028/NIST.FIPS.140-3>
- FIPS140-3_IG** **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
August 2023
<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements>
- FIPS180-4** **Secure Hash Standard (SHS)**
March 2012
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>
- FIPS186-5** **Digital Signature Standard (DSS)**
February 2023
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>
- FIPS197** **Advanced Encryption Standard**
November 2001
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- FIPS198-1** **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
- PKCS#1** **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**
February 2003
<http://www.ietf.org/rfc/rfc3447.txt>
- SP800-38A** **Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
<http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- SP800-38B** **NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**
May 2005
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
- SP800-38C** **NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
May 2004
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf>

SP800-38D	NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP800-38F	NIST Special Publication 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping December 2012 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP800-38G	NIST Special Publication 800-38G - Recommendation for Block Cipher Modes of Operation: Methods for Format - Preserving Encryption March 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf
SP800-56Arev3	NIST Special Publication 800-56A Revision 2 - Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography May 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
SP800-90Arev1	NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-90B	(Second DRAFT) NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation January 2016 http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
SP800-131Arev1	NIST Special Publication 800-131A Revision 1- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths November 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
SP800-133rev2	NIST Special Publication 800-133rev2 - Recommendation for Cryptographic Key Generation June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP800-135rev1	NIST Special Publication 800-135 Revision 1 - Recommendation for Existing Application-Specific Key Derivation Functions December 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf