ORACLE
Linux

FIPS 140-3 Non-Proprietary Security Policy

Oracle Corporation

Oracle Linux 9 OpenSSL FIPS Provider

Software Version: 3.0.7-b27cdeb3ba51be46

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

Title: Oracle Linux 9 OpenSSL FIPS Provider Security Policy

Date: July 29th, 2025

Contributing Authors:

Oracle Linux Engineering

Security Evaluations – Global Product Security

atsec information security

Oracle Corporation

World Headquarters

2300 Oracle Way

Austin, TX 78741

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

www.oracle.com

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

ORACLE

Table of Contents

ORACLE

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for software version 3.0.7-b27cdeb3ba51be46, package version openssl-libs-3.0.7-24.0.3.el9_fips, of the Oracle Linux 9 OpenSSL FIPS Provider. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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

1.1.1. How This Security Policy was Prepared

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

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The Oracle Linux 9 OpenSSL FIPS Provider (hereafter referred to as "the module") is defined as a software module in a multi-chip standalone embodiment. It provides a C language application program interface (API) for use by other applications that require cryptographic functionality. The module consists of one software component, the "FIPS provider", which implements the FIPS requirements, and the cryptographic functionality provided to the operator.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

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).

Tested Operational Environment's Physical Perimeter (TOEPP):

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

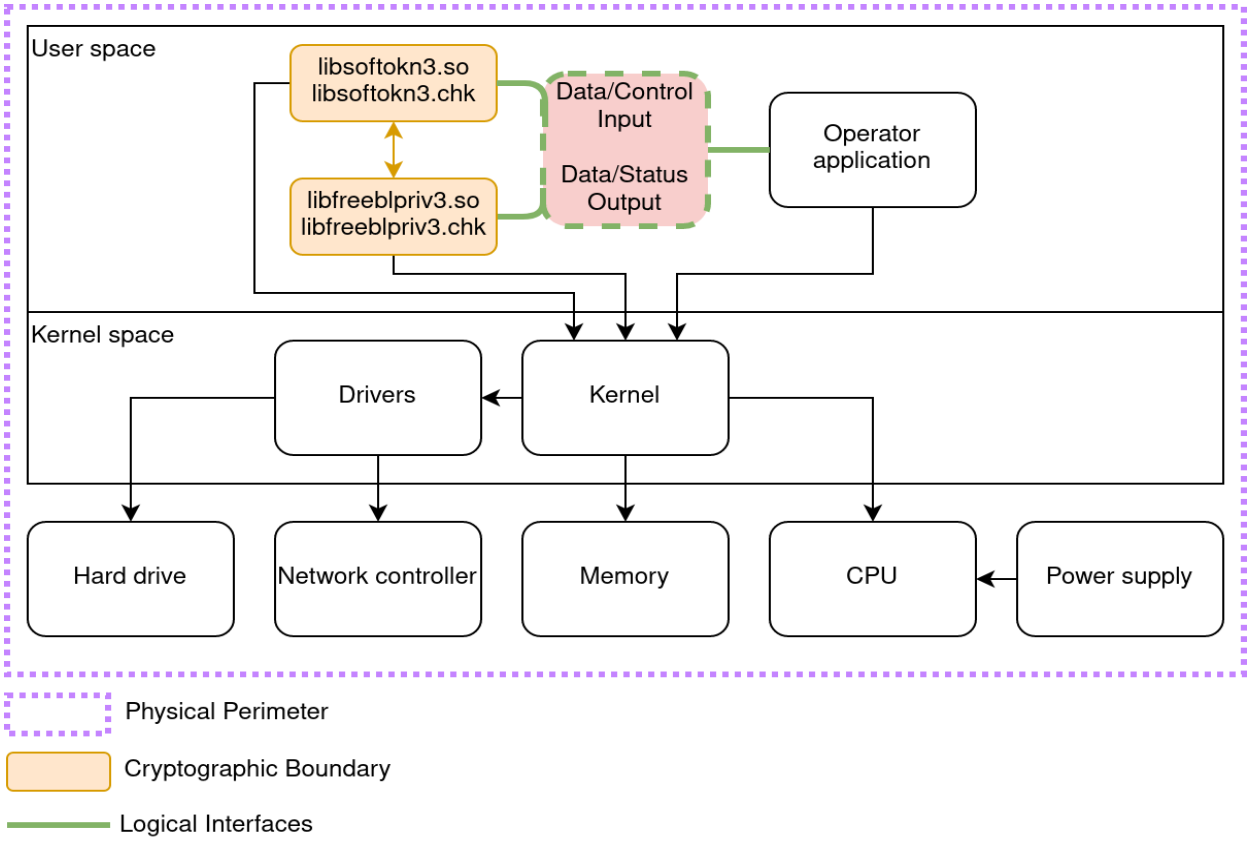

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips.so on ORACLE SERVER X9-2c with Intel(R) Xeon(R) Platinum 8358	3.0.7-b27cdeb3ba51be46	N/A	HMAC-SHA-256
fips.so on ORACLE SERVER E4-2c with AMD EPYC 7J13	3.0.7-b27cdeb3ba51be46	N/A	HMAC-SHA-256
fips.so on ORACLE SERVER A1-2c with Ampere(R) Altra(R) Q80-30	3.0.7-b27cdeb3ba51be46	N/A	HMAC-SHA-256
fips.so on Marvell Liquid IO II (MIPS64) SmartNIC with OCTEON III	3.0.7-b27cdeb3ba51be46	N/A	HMAC-SHA-256

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

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Oracle Linux 9	ORACLE SERVER X9-2c	Intel(R) Xeon(R) Platinum 8358	Yes	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	ORACLE SERVER E4-2c	AMD EPYC 7J13	Yes	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	ORACLE SERVER A1-2c	Ampere(R) Altra(R) Q80-30	Yes	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	ORACLE SERVER X9-2c	Intel(R) Xeon(R) Platinum 8358	No	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	ORACLE SERVER E4-2c	AMD EPYC 7J13	No	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	ORACLE SERVER A1-2c	Ampere(R) Altra(R) Q80-30	No	KVM on Oracle Linux 8	3.0.7-b27cdeb3ba51be46
Oracle Linux 9	Marvell Liquid IO II (MIPS64) SmartNIC	OCTEON III	No	N/A	3.0.7-b27cdeb3ba51be46

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

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

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

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

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

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service as defined in section 4.3
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Not required per IG 2.4.C

Table 5: Modes List and Description

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode. The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

Mode Change Instructions and Status:

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

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CBC-CS1	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CBC-CS2	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CBC-CS3	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CCM	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38C
AES-CFB1	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CFB128	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CFB8	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-CMAC	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38B
AES-CTR	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-ECB	A4313, A4314, A4315, A4320, A4327, A4328, A4329, A4331, A4332, A4333, A4334	-	SP 800-38A
AES-GCM	A4316, A4321, A4322, A4323, A4335, A4336, A4337, A4338, A4339, A4340, A4341, A4342, A4343	-	SP 800-38D
AES-GMAC	A4316, A4321, A4322, A4323, A4335, A4336, A4337, A4338, A4339, A4340, A4341, A4342, A4343	-	SP 800-38D
AES-KW	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38F
AES-KWP	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38F
AES-OFB	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38A
AES-XTS Testing Revision 2.0	A4313, A4314, A4315, A4327, A4328, A4329	-	SP 800-38E
Counter DRBG	A4311	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-4)	A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
Hash DRBG	A4311	-	SP 800-90A Rev. 1
HMAC DRBG	A4311	-	SP 800-90A Rev. 1
HMAC-SHA-1	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-224	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-256	A4317, A4318, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-384	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-512	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-512/224	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA2-512/256	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 198-1
HMAC-SHA3-224	A4312, A4319	-	FIPS 198-1
HMAC-SHA3-256	A4312, A4319	-	FIPS 198-1
HMAC-SHA3-384	A4312, A4319	-	FIPS 198-1
HMAC-SHA3-512	A4312, A4319	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4317, A4326, A4330, A4344, A4345, A4346	-	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4325	-	SP 800-56A Rev. 3
KDA HKDF Sp800-56Cr1	A4310	-	SP 800-56C Rev. 2
KDA OneStep SP800-56Cr2	A4309	-	SP 800-56C Rev. 2
KDA TwoStep SP800-56Cr2	A4309	-	SP 800-56C Rev. 2
KDF ANS 9.42 (CVL)	A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346	-	SP 800-135 Rev. 1
KDF ANS 9.63 (CVL)	A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346	-	SP 800-135 Rev. 1
KDF SP800-108	A4324	-	SP 800-108 Rev. 1
KDF SSH (CVL)	A4320, A4326, A4331, A4332, A4333, A4334	-	SP 800-135 Rev. 1
PBKDF	A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346	-	SP 800-132
RSA KeyGen (FIPS186-4)	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
RSA SigGen (FIPS186-4)	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 186-4
Safe Primes Key Generation	A4325	-	SP 800-56A Rev. 3
Safe Primes Key Verification	A4325	-	SP 800-56A Rev. 3
SHA-1	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA2-224	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA2-256	A4317, A4318, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA2-512	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA2-512/224	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA2-512/256	A4317, A4326, A4330, A4344, A4345, A4346	-	FIPS 180-4
SHA3-224	A4312, A4319	-	FIPS 202
SHA3-256	A4312, A4319	-	FIPS 202
SHA3-384	A4312, A4319	-	FIPS 202
SHA3-512	A4312, A4319	-	FIPS 202
SHAKE-128	A4312, A4319	-	FIPS 202
SHAKE-256	A4312, A4319	-	FIPS 202
TLS v1.2 KDF RFC7627 (CVL)	A4317, A4326, A4330, A4344, A4345, A4346	-	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A4310	-	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Cryptographic Key Generation (CKG)	Key Type:Asymmetric RSA:2048, 3072, 4096 bits with 112, 128, 149 bits of key strength. ECDSA:P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of key strength Safe Primes Key Generation:2048, 3072, 4096, 6144, 8192-bit keys with 112-200 bits of key strength	N/A	SP 800-133Rev2 section 4, example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

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

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The module does not implement non-approved algorithms allowed in the approved mode of operation with no security claimed.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES GCM (external IV)	Encryption
ANS X9.42 KDF (SHAKE128, SHAKE256)	ANS X9.42 Key Derivation
ANS X9.63 KDF (SHA-1, SHAKE128, SHAKE256)	ANS X9.63 Key Derivation
Hash_DRBG (SHA2-224, SHA2-384)	Random Number Generation
HMAC_DRBG (SHA2-224, SHA2-384)	Random Number Generation
ECDSA with curve P-192	Key Pair Generation, Key Pair Verification
HMAC (< 112-bit keys)	Message Authentication HMAC
KAS1, KAS2	Shared Secret Computation
KBKDF (< 112-bit keys)	Key-Based Key Derivation

Name	Use and Function
KDA OneStep (< 112-bit keys)	KDA OneStep Key Derivation
HKDF (< 112-bit keys)	HKDF Key Derivation
ANS X9.42 KDF (< 112-bit keys)	ANS X9.42 Key Derivation
ANS X9.63 KDF (< 112-bit keys)	ANS X9.63 Key Derivation
KDA OneStep (SHAKE128, SHAKE256)	KDA OneStep Key Derivation
HKDF (SHAKE128, SHAKE256)	HKDF OneStep Key Derivation
PBKDF2 (short password; short salt; insufficient iterations; < 112-bit keys)	Password-Based Key Derivation
RSA and ECDSA (pre-hashed message), ECDSA with curve P-192	Signature Generation, Signature Verification
RSA-PSS (invalid salt length)	Signature Generation, Signature Verification
RSA-OAEP	Asymmetric Encryption, Asymmetric Decryption
SSH KDF (SHA2-512/224, SHA2-512/256, SHA-3, SHAKE128, SHAKE256)	SSH Key Derivation
TLS 1.2 KDF (SHA-1, SHA2-224, SHA2-512/224, SHA2-512/256, SHA-3)	TLS 1.2 Key Derivation
TLS 1.2 KDF using master secret non-compliant with RFC 7627	TLS v1.2 Key Derivation
TLS 1.3 KDF (SHA-1, SHA2-224, SHA2-512, SHA2-512/224, SHA2-512/256, SHA-3)	TLS v1.3 Key Derivation
KDA TwoStep (< 112-bit keys)	KDA TwoStep Key Derivation
KDA TwoStep (SHAKE128, SHAKE256)	KDA TwoStep Key Derivation
SSH KDF (< 112-bit keys)	SSH Key Derivation

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KDA OneStep Key Derivation	KAS-56CKDF	Key Derivation		KDA OneStep SP800-56Cr2: (A4309)
KDA TwoStep Key Derivation	KAS-56CKDF	Key Derivation		KDA TwoStep SP800-56Cr2: (A4309)
HKDF Key Derivation	KAS-56CKDF	Key Derivation		KDA HKDF Sp800-56Cr1: (A4310)
TLS v1.3 Key Derivation	KAS-135KDF	Key Derivation		TLS v1.3 KDF: (A4310)
ANS X9.42 Key Derivation	KAS-135KDF	Key Derivation		KDF ANS 9.42: (A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346)
ANS X9.63 Key Derivation	KAS-135KDF	Key Derivation		KDF ANS 9.63: (A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346)
TLS v1.2 Key Derivation	KAS-135KDF	Key Derivation		TLS v1.2 KDF RFC7627: (A4317, A4326, A4330, A4344, A4345, A4346)
Random Number Generation	DRBG	Random Number Generation		Counter DRBG: (A4311) HMAC DRBG: (A4311) Hash DRBG: (A4311)
Signature Generation	DigSig-SigGen	Signature Generation		ECDSA SigGen (FIPS186-4): (A4312, A4317, A4319, A4326, A4330, A4344, A4345,

Name	Type	Description	Properties	Algorithms
				A4346) RSA SigGen (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346)
Signature Verification	DigSig-SigVer	Signature Verification		ECDSA SigVer (FIPS186-4): (A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346) RSA SigVer (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346)
Message Authentication HMAC	MAC	Message Authentication Code Generation, Message Authentication Code Verification		HMAC-SHA3-224: (A4312, A4319) HMAC-SHA3-256: (A4312, A4319) HMAC-SHA3-384: (A4312, A4319) HMAC-SHA3-512: (A4312, A4319) HMAC-SHA-1: (A4317, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-224: (A4317, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-256: (A4317, A4318, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-384: (A4317, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-512: (A4317, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-512/224: (A4317, A4326, A4330, A4344, A4345, A4346) HMAC-SHA2-512/256: (A4317, A4326, A4330, A4344, A4345, A4346)
Message Authentication CMAC/GMAC	MAC	Message Authentication Code Generation, Message Authentication Code Verification		AES-GMAC: (A4316, A4321, A4322, A4323, A4335, A4336, A4337, A4338, A4339, A4340, A4341, A4342, A4343) AES-CMAC: (A4313,

Name	Type	Description	Properties	Algorithms
				A4314, A4315, A4327, A4328, A4329)
Password-Based Key Derivation	PBKDF	Password-Based Key Derivation		PBKDF: (A4312, A4317, A4319, A4326, A4330, A4344, A4345, A4346)
Message Digest	SHA XOF	Message Digest		SHA3-224: (A4312, A4319) SHA3-256: (A4312, A4319) SHA3-384: (A4312, A4319) SHA3-512: (A4312, A4319) SHAKE-128: (A4312, A4319) SHAKE-256: (A4312, A4319) SHA-1: (A4317, A4326, A4330, A4344, A4345, A4346) SHA2-224: (A4317, A4326, A4330, A4344, A4345, A4346) SHA2-256: (A4317, A4318, A4326, A4330, A4344, A4345, A4346) SHA2-384: (A4317, A4326, A4330, A4344, A4345, A4346) SHA2-512: (A4317, A4326, A4330, A4344, A4345, A4346) SHA2-512/224: (A4317, A4326, A4330, A4344, A4345, A4346) SHA2-512/256: (A4317, A4326, A4330, A4344, A4345, A4346)
Encryption	BC-UnAuth	Encryption		AES-CBC: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS1: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS2: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS3: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CFB1: (A4313,

Name	Type	Description	Properties	Algorithms
				A4314, A4315, A4327, A4328, A4329) AES-CFB128: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CFB8: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CTR: (A4313, A4314, A4315, A4327, A4328, A4329) AES-ECB: (A4313, A4314, A4315, A4320, A4327, A4328, A4329, A4331, A4332, A4333, A4334) AES-OFB: (A4313, A4314, A4315, A4327, A4328, A4329) AES-XTS Testing Revision 2.0: (A4313, A4314, A4315, A4327, A4328, A4329)
Decryption	BC-UnAuth	Decryption		AES-CBC: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS1: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS2: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CBC-CS3: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CFB1: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CFB128: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CFB8: (A4313, A4314, A4315, A4327, A4328, A4329) AES-CTR: (A4313, A4314, A4315, A4327, A4328, A4329) AES-ECB: (A4313, A4314, A4315, A4320, A4327, A4328, A4329, A4331, A4332, A4333,

Name	Type	Description	Properties	Algorithms
				A4334) AES-OFB: (A4313, A4314, A4315, A4327, A4328, A4329) AES-XTS Testing Revision 2.0: (A4313, A4314, A4315, A4327, A4328, A4329)
Authenticated Encryption	BC-Auth	Authenticated Encryption		AES-CCM: (A4313, A4314, A4315, A4327, A4328, A4329) AES-GCM: (A4316, A4321, A4322, A4323, A4335, A4336, A4337, A4338, A4339, A4340, A4341, A4342, A4343) AES-KW: (A4313, A4314, A4315, A4327, A4328, A4329) AES-KWP: (A4313, A4314, A4315, A4327, A4328, A4329)
Authenticated Decryption	BC-Auth	Authenticated Decryption		AES-CCM: (A4313, A4314, A4315, A4327, A4328, A4329) AES-GCM: (A4316, A4321, A4322, A4323, A4335, A4336, A4337, A4338, A4339, A4340, A4341, A4342, A4343) AES-KW: (A4313, A4314, A4315, A4327, A4328, A4329) AES-KWP: (A4313, A4314, A4315, A4327, A4328, A4329)
Key Pair Generation	AsymKeyPair-KeyGen CKG	Key Pair Generation		ECDSA KeyGen (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346) RSA KeyGen (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346) Safe Primes Key Generation: (A4325) Cryptographic Key Generation (CKG): () Key Type: Asymmetric RSA: 2048, 3072, 4096 bits with 112, 128, 149

Name	Type	Description	Properties	Algorithms
				bits of key strength. ECDSA: P-224, P-256, P-384, P-521 elliptic curves with 112-256 bits of key strength Safe Primes Key Generation: 2048, 3072, 4096, 6144, 8192-bit keys with 112-200 bits of key strength
Key Pair Verification	AsymKeyPair-KeyVer	Key Pair Verification		ECDSA KeyVer (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346) Safe Primes Key Verification: (A4325)
Shared Secret Computation	KAS-SSC	Shared Secret Computation; Compliant with IG D.F scenario 2(1)		KAS-ECC-SSC Sp800-56Ar3: (A4317, A4326, A4345, A4346, A4330, A4344) KAS-FFC-SSC Sp800-56Ar3: (A4325)
Key-Based Key Derivation	KBKDF	Key Derivation		KDF SP800-108: (A4324)
SSH Key Derivation	KAS-135KDF	Key Derivation		KDF SSH: (A4320, A4326, A4331, A4332, A4333, A4334)
Signature Verification (Legacy)	DigSig-SigVer	Legacy digital signature verification	Publications:FIPS 140-3 IG C.M legacy algorithms RSA Keys:1024 bits with 80 bits of security	RSA SigVer (FIPS186-4): (A4317, A4326, A4330, A4344, A4345, A4346)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV

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

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

The module does not implement the TLS protocol. The module's implementation of AES GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the counter (the nonce_explicit part of the IV) does not exhaust the maximum number of possible values for a given session key.

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

Alternatively, the Crypto Officer can use the module's API to perform AES GCM encryption using internal IV generation. These IVs are always 96 bits and generated using the approved DRBG internal to the module's boundary, compliant with Scenario 2 of FIPS 140-3 IG C.H.

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

Finally, for TLS 1.3, the AES GCM implementation uses the context of Scenario 5 of FIPS 140-3 IG C.H. The protocol that provides this compliance is TLS 1.3, defined in RFC8446 of August 2018, using the cipher-suites that explicitly select AES GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The module supports acceptable AES GCM cipher suites from Section 3.3.1 of SP800-52r2. TLS 1.3 employs separate 64-bit sequence numbers, one for protocol records that are received, and one for protocol records that are sent to a peer. These sequence numbers are set at zero at the beginning of a TLS 1.3 connection and each time when the AES-GCM key is changed. After reading or writing a record, the respective sequence number is incremented by one. The protocol specification determines that the sequence number should not wrap, and if this condition is observed, then the protocol implementation must either trigger a re-key of the session (i.e., a new key for AES-GCM), or terminate the connection.

2.7.2 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 length of the password or passphrase shall be at least 8 characters, and shall consist of lowercase, uppercase, and numeric characters. The probability of guessing the value is estimated to be at most 10^{-8}. Combined with the minimum iteration count as described below, this provides an acceptable trade-off between user experience and security against brute-force attacks.
- A portion of the salt, with a length of at least 128 bits (this is verified by the module to determine the service is approved), shall be generated randomly using the SP 800-90Ar1 DRBG provided by the module.
- The iteration count shall be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The module only allows minimum iteration count to be 1000.

2.7.3 AES XTS

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

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

2.7.4 SP 800-56Ar3 Assurances

The module offers DH and ECDH shared secret computation services compliant to the SP 800-56Ar3 and meeting IG D.F scenario 2 path (1). To meet the required assurances listed in section 5.6 of SP 800-56Ar3, 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 module's "Key pair generation" service for generating DH/ECDH ephemeral keys. This meets the assurances required by key pair owner defined in the section 5.6.2.1 of SP 800-56Ar3.
- As part of the module's shared secret computation (SSC) service, the module internally performs the public key validation 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 800-56Ar3.
- The module does not support static keys therefore the "assurance of peer's possession of private key" is not applicable.

2.7.5 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.

2.7.6 KAS-SSC

The module offers as a service to an external operator (e.g., calling application) CAVP-tested KAS SSC that map to IG D.F Scenario 2 path (1) without establishing a module key/SSP used by the module for cryptographic protection. The module offers KAS-ECC-SSC as a service that receives as inputs all keying material necessary to compute and output the shared secret without applying a KDF/KDA which is a separate module service.

2.7.7 SHA-1

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

2.7.8 RSA

All supported modulus sizes for RSA signature verification have been CAVP tested. CAVP testing performed on the module's legacy implementations, specifically digital signature verification using SHA-1 or with 1024-bits modulus, were not testable under FIPS 186-5, but have been tested under FIPS 186-4 per IG C.K additional comment 2.

2.8 RBG and Entropy

Cert Number	Vendor Name
E90	Oracle Corp

Table 10: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
OpenSSL CPU Time Jitter	Non-Physical	Oracle Linux 9 on Oracle SERVER X9-2c; Oracle Linux 9 on ORACLE SERVER E4-2c; Oracle Linux 9 on ORACLE SERVER A1-2c	256	256	LFSR, HMAC_DRBG_SHA2-512(A4162), ctrDRBG AES-256(A4311)

Table 11: Entropy Sources

RNG Information:

The module employs two Deterministic Random Bit Generator (DRBG) implementations based on SP 800-90Ar1. These DRBGs are used internally by the module (e.g. to generate seeds for asymmetric key pairs and random numbers for security functions). They can also be accessed using the specified API functions. The following parameters are used:

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

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

2.9 Key Generation

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

2.10 Key Establishment

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

2.11 Industry Protocols

For DH, the module supports the use of the safe primes defined in RFC 3526 (IKE) and RFC 7919 (TLS) as listed above. Note that the module only implements key pair generation, key pair verification, and shared secret computation. No other part of the IKE or TLS protocols is implemented (with the exception of the TLS 1.2 and 1.3 KDFs).

SSH KDF, TLS 1.2 KDF (RFC 7627), TLS 1.3 KDF implementations shall only be used to generate secret keys in the context of the SSH, TLS 1.2, or TLS 1.3 protocols, respectively. Note that TLS 1.2 KDF must be compliant with RFC 7627 to be considered approved.

ANS X9.42 KDF and ANS X9.63 KDF implementations shall only be used to generate secret keys in the context of an ANS X9.42-2001 resp. ANS X9.63-2001 key agreement scheme.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 12: Ports and Interfaces

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

The module does not implement the control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement authentication.

4.2 Roles

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

Table 13: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Digest	Compute a message digest	EVP_DigestFinal_ex returns 1	Message	Message digest	Message Digest	Crypto Officer
XOF	Compute the output of an XOF	EVP_DigestFinalXOF returns 1	Message	Message digest	Message Digest	Crypto Officer
Encryption	Encrypt a plaintext	EVP_EncryptFinal_ex returns 1	AES Key, plaintext, IV	Ciphertext	Encryption Decryption	Crypto Officer - AES Key: W,E
Decryption	Decrypt a ciphertext	EVP_DecryptFinal_ex returns 1	AES Key, ciphertext, IV	Plaintext	Encryption Decryption	Crypto Officer - AES Key: W,E
Authenticated Encryption	Encrypt a plaintext	AES GCM:EVP_CIPHER_*_FIPS_INDICATOR_APPROVED Others: EVP_EncryptFinal_ex returns 1	AES key, plaintext	Ciphertext, MAC tag	Authenticated Encryption	Crypto Officer - AES Key: W,E
Authenticated Decryption	Decrypt a ciphertext	AES GCM:EVP_CIPHER_*_FIPS_INDICATOR_APPROVED Others: EVP_DecryptFinal_ex returns 1	AES Key, ciphertext	Plaintext or failure	Authenticated Decryption	Crypto Officer - AES Key: W,E
AES Message Authentication	Compute a MAC tag	HMAC:EVP_MAC_*_FIPS_INDICATOR_APPROVED Others: EVP_MAC_final returns 1	AES Key, message	MAC tag	Message Authentication CMAC/GMAC	Crypto Officer - AES Key: W,E
HMAC Message Authentication	Compute a MAC tag	HMAC:EVP_MAC_*_FIPS_INDICATOR_APPROVED Others: EVP_MAC_final returns 1	HMAC Key, message	MAC tag	Message Authentication HMAC	Crypto Officer - HMAC Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Shared Secret Computation	Compute a shared secret Compliant with: Scenario 2 (1) of FIPS 140-3 IG D.F: Shared secret computation	EVP_PKEY_derive returns 1	DH Private Key(owner), DH Public Key(peer) EC Private Key(owner), EC Public Key(peer)	Shared secret	Shared Secret Computation	Crypto Officer - DH Private Key: W,E - DH Public Key: W,E - EC Private Key: W,E - EC Public Key: W,E - Shared Secret: G,R
KDA OneStep Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	KDA OneStep derived Key	KDA OneStep Key Derivation	Crypto Officer - Shared Secret: W,E - KDA OneStep Derived Key: G,R
KDA TwoStep Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	KDA TwoStep derived key	KDA TwoStep Key Derivation	Crypto Officer - Shared Secret: W,E - KDA TwoStep Derived Key: G,R
HKDF Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	HKDF derived key	HKDF Key Derivation	Crypto Officer - Shared Secret: W,E - HKDF Derived Key: G,R
SSH Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	SSH derived key	SSH Key Derivation	Crypto Officer - Shared Secret: W,E - SSH KDF Derived Key: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
KBKDF Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	KBKDF derived key	Key-Based Key Derivation	Crypto Officer - Shared Secret: W,E - KBKDF Derived Key: G,R
TLS 1.2 Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	TLS 1.2 derived key	TLS v1.2 Key Derivation	Crypto Officer - Shared Secret: W,E - TLS 1.2 Derived Secret: G,R
ANS X9.63 Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	ANS X9.63 derived key	ANS X9.63 Key Derivation	Crypto Officer - Shared Secret: W,E - ANS X9.63 KDF Derived key: G,R
TLS v1.3 Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	TLS v1.3 derived key	TLS v1.3 Key Derivation	Crypto Officer - Shared Secret: W,E - TLS 1.3 Derived Secret: G,R
ANS X9.42 Key Derivation	Derive a key	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Shared Secret	ANS X9.42 derived key	ANS X9.42 Key Derivation	Crypto Officer - Shared Secret: W,E - ANS X9.42 KDF Derived Key: G,R
Password-Based Key Derivation	Derive a key from a password	EVP_KDF_*_FIPS_INDICATOR_APPROVED	Password	PBKDF derived key	Password-Based Key Derivation	Crypto Officer - Password: W,E - PBKDF2 Derived Key: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
DH Key Pair Generation	Key Pair Generation	EVP_PKEY_generate returns 1	DH Group	Module generated DH private key, Module generated DH public key	Key Pair Generation	Crypto Officer - Module Generated DH Public Key: G,R - Module Generated DH Private Key: G,R - Intermediate Key Generation Value: G,E,Z
EC Key Pair Generation	Key Pair Generation	EVP_PKEY_generate returns 1	Curve	Module generated EC private key, Module generated EC public key	Key Pair Generation	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 Pair Generation	Key Pair Generation	EVP_PKEY_generate returns 1	Modulus	Module generated RSA private key, Module generated RSA public key	Key Pair Generation	Crypto Officer - Module Generated RSA Private Key: G,R - Module Generated RSA Public Key: G,R - Intermediate Key Generation Value: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Public Key Verification	Verify an EC public key	EVP_PKEY_public_check EVP_PKEY_private_check EVP_PKEY_check returns 1	EC public key	Return codes/log messages	Key Pair Verification	Crypto Officer - EC Private Key: W,E - EC Public Key: W,E
Random Number Generation	Generate random bytes	EVP_RAND_generate returns 1	Output length	Random bytes	Random Number Generation	Crypto Officer - Entropy Input: W,E - DRBG Seed: G,E - Internal State (V, Key): G,E
Signature Verification	Verify a digital signature	RSA: OSSL_*_FIPSINDICATOR_APPROVED and EVP_SIGNATURE_*_FIPS_INDICATOR_APPROVED ECDSA: OSSL_*_FIPSINDICATOR_APPROVED	Message, EC Public Key or RSA Public Key, signature, hash algorithm	Pass/fail	Signature Verification Signature Verification (Legacy)	Crypto Officer - EC Public Key: W,E - RSA Public Key: W,E
Signature Generation	Signature Generation	RSA: OSSL_*_FIPSINDICATOR_APPROVED and EVP_SIGNATURE_*_FIPS_INDICATOR_APPROVED ECDSA: OSSL_*_FIPSINDICATOR_APPROVED	Message, EC Private Key or RSA Private Key, hash algorithm	Signature	Signature Generation	Crypto Officer - EC Private Key: W,E - RSA Private Key: W,E
Show Version	Return the module name and version information	None	N/A	Module name and version	None	Crypto Officer
Show Status	Return the module status	None	N/A	Module status	None	Crypto Officer
Self-Test	Perform the CASTs and integrity tests	None	N/A	Pass/Fail		Crypto Officer
Zeroization	Zeroize all SSPs	None	Any SSP	N/A	None	Crypto Officer - AES Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - HMAC Key: Z - Shared Secret: Z - Password: Z - PBKDF2 Derived Key: Z - KDA OneStep Derived Key: Z - ANS X9.42 KDF Derived Key: Z - ANS X9.63 KDF Derived key: Z - SSH KDF Derived Key: Z - Entropy Input: Z - DRBG Seed: Z - Internal State (V, Key): Z - Internal State (V, C): Z - DH Public Key: Z - DH Private Key: Z - Module Generated DH Public Key: Z - Module Generated DH Private Key: Z - EC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - EC Public Key: Z - Module Generated EC Private Key: Z - Module Generated EC Public Key: Z - RSA Private Key: Z - RSA Public Key: Z - Module Generated RSA Private Key: Z - Module Generated RSA Public Key: Z - Intermediate Key Generation Value: Z - TLS 1.2 Derived Secret: Z - TLS 1.3 Derived Secret: Z - HKDF Derived Key: Z

Table 14: Approved Services

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

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

- **Zeroize (Z)**: The module zeroizes the SSP.

To interact with the module, a calling application must use the EVP API layer provided by OpenSSL. This layer will delegate the request to the FIPS provider, which will in turn perform the requested service. Additionally, this EVP API layer can be used to retrieve the approved service indicator for the module. The redhat_ossl_query_fipsindicator() function indicates whether an EVP API function is approved. After a cryptographic service was performed by the module, the API context associated with this request can contain a parameter (listed below) which represents the service indicator returned by the function. When the cryptographic service is approved, the function returns an indicator value of 1; when it is non-approved, the value is 0.

- OSSL_CIPHER_PARAM_*_FIPS_INDICATOR
- OSSL_MAC_PARAM_*_FIPS_INDICATOR
- OSSL_KDF_PARAM_*_FIPS_INDICATOR
- OSSL_SIGNATURE_PARAM_*_FIPS_INDICATOR
- OSSL_ASYM_CIPHER_PARAM_*_FIPS_INDICATOR

4.4 Non-Approved Services

Name	Description	Algorithms	Role
AES GCM (external IV)	Encryption	AES GCM (external IV)	CO
ANS X9.42 KDF (SHAKE128, SHAKE256)	Key Derivation	ANS X9.42 KDF (SHAKE128, SHAKE256)	CO
ANS X9.63 KDF (SHA-1, SHAKE128, SHAKE256)	Key Derivation	ANS X9.63 KDF (SHA-1, SHAKE128, SHAKE256)	CO
Hash_DRBG (SHA2-224, SHA2-384)	Random Number Generation	Hash_DRBG (SHA2-224, SHA2-384)	CO
HMAC_DRBG (SHA2-224, SHA2-384)	Random Number Generation	HMAC_DRBG (SHA2-224, SHA2-384)	CO
ECDSA with curve P-192	Key Pair Generation, Key Pair Verification	ECDSA with curve P-192	CO
HMAC (< 112-bit keys)	Message Authentication	HMAC (< 112-bit keys)	CO
KAS1, KAS2	Shared Secret Computation	KAS1, KAS2	CO
KBKDF, KDA OneStep, KDA TwoStep, HKDF, ANS X9.42 KDF, ANS X9.63 KDF (< 112-bit keys)	Key Derivation	KBKDF (< 112-bit keys) KDA OneStep (< 112-bit keys) HKDF (< 112-bit keys) ANS X9.42 KDF (< 112-bit keys) ANS X9.63 KDF (< 112-bit keys) KDA TwoStep (< 112-bit keys)	CO
KDA OneStep, KDA TwoStep, HKDF (SHAKE128, SHAKE256)	Key Derivation	KDA OneStep (SHAKE128, SHAKE256) HKDF (SHAKE128, SHAKE256) KDA TwoStep (SHAKE128, SHAKE256)	CO
PBKDF2 (short password; short salt; insufficient iterations; < 112-bit keys)	Password-Based Key Derivation	PBKDF2 (short password; short salt; insufficient iterations; < 112-bit keys)	CO
RSA and ECDSA (pre-hashed message), ECDSA with curve P-192	Signature Generation, Signature Verification	RSA and ECDSA (pre-hashed message), ECDSA with curve P-192	CO
RSA-PSS (invalid salt length)	Signature Generation, Signature Verification	RSA-PSS (invalid salt length)	CO
RSA-OAEP	Asymmetric Encryption, Asymmetric Decryption	RSA-OAEP	CO
SSH KDF (SHA2-512/224, SHA2-512/256, SHA-3, SHAKE128, SHAKE256, < 112-bit keys)	SSH Key Derivation	SSH KDF (SHA2-512/224, SHA2-512/256, SHA-3, SHAKE128, SHAKE256) SSH KDF (< 112-bit keys)	CO

Name	Description	Algorithms	Role
TLS 1.2 KDF (SHA-1, SHA2-224, SHA2-512/224, SHA2-512/256, SHA-3)	Key Derivation	TLS 1.2 KDF (SHA-1, SHA2-224, SHA2-512/224, SHA2-512/256, SHA-3)	CO
TLS 1.2 KDF using master secret non-compliant with RFC 7627	Key Derivation	TLS 1.2 KDF using master secret non-compliant with RFC 7627	CO
TLS 1.3 KDF (SHA-1, SHA2-224, SHA2-512, SHA2-512/224, SHA2-512/256, SHA-3)	Key Derivation	TLS 1.3 KDF (SHA-1, SHA2-224, SHA2-512, SHA2-512/224, SHA2-512/256, SHA-3)	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing a HMAC SHA-256 value calculated at run time with the HMAC SHA-256 value embedded in the fips.so file that was computed at build time. If the integrity test fails, the module enters the error state. The HMAC key for the integrity verification is embedded in the module.

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

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

6.2 Configuration Settings and Restrictions

The module shall be installed as stated in Section 11.1.

There are no concurrent operators.

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

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

7 Physical Security

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 16: Storage Areas

SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls, as specified in Section 9.3.

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.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Calling the zeroization API	Zeroizes the SSPs	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. All data output is inhibited during zeroization.	By calling the appropriate zeroization functions: AES key: EVP_CIPHER_CTX_free, EVP_MAC_CTX_free HMAC key: EVP_MAC_CTX_free Key-derivation key: EVP_KDF_CTX_free Shared secret: EVP_KDF_CTX_free PBKDF Password: EVP_KDF_CTX_free Derived key: EVP_KDF_CTX_free Entropy input: EVP_RAND_CTX_free DRBG seed: EVP_RAND_CTX_free DRBG Internal state: EVP_RAND_CTX_free DH private key: EVP_PKEY_free DH public key: EVP_PKEY_free EC private key: EVP_PKEY_free EC public key: EVP_PKEY_free RSA private key: EVP_PKEY_free RSA public key: EVP_PKEY_free TLS derived secret: EVP_KDF_CTX_free

Zeroization Method	Description	Rationale	Operator Initiation
Automatic	Zeroizes the SSPs	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable. All data output is inhibited during zeroization.	Intermediate key generation value: zeroized automatically by the module (after the requested service completed)
Remove power from the module	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By removing power

Table 18: SSP Zeroization Methods

All data output is inhibited during zeroization. Memory is deallocated after zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES key used for encryption, decryption, authenticated encryption, authenticated decryption and computing MAC tags	128-256 bits - 128-256 bits	Symmetric key - CSP			Message Authentication CMAC/GMAC Encryption Decryption Authenticated Encryption Authenticated Decryption
HMAC Key	HMAC Key	112-256 bits - 112-256 bits	Authentication key - CSP			Message Authentication HMAC
Shared Secret	Shared secret generated by DH/ECDH	ECDH: 128-256 bits; DH: 112-200 bits - ECDH: 128-256 bits; DH: 112-200 bits	Shared secret - CSP		Shared Secret Computation	Shared Secret Computation HKDF Key Derivation ANS X9.42 Key Derivation ANS X9.63 Key Derivation Key-Based Key Derivation TLS v1.2 Key Derivation TLS v1.3 Key Derivation
Password	PBKDF password	at least 8 characters - N/A	Password - CSP			Password-Based Key Derivation
PBKDF2 Derived Key	PBKDF2 derived key	112-4096 bits - 112-256 bits	Derived Key - CSP	Password-Based Key Derivation		
KDA OneStep Derived Key	KDA OneStep derived key	112-2048 bits - 112-256 bits	Derived Key - CSP	KDA OneStep Key Derivation		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KDA TwoStep Derived Key	KDA TwoStep derived key	112-2048 bits - 112-256 bits	Derived Key - CSP	KDA TwoStep Key Derivation		
ANS X9.42 KDF Derived Key	ANS X9.42 KDF derived key	112-4096 bits - 112-256 bits	Derived Key - CSP	ANS X9.42 Key Derivation		
ANS X9.63 KDF Derived key	ANS X9.63 KDF Derived key	112-4096 bits - 112-256 bits	Derived Key - CSP	ANS X9.63 Key Derivation		
SSH KDF Derived Key	PBKDF2 derived key	112-1024 bits - 112-256 bits	Derived Key - CSP	SSH Key Derivation		
Entropy Input	(compliant with IG D.L) Entropy input used to seed the DRBGs	128-448 bits - 128-256 bits	Entropy - CSP			Random Number Generation
DRBG Seed	(compliant with IG D.L) DRBG seed derived from entropy input as defined in SP 800-90Ar1	256, 320, 384 bits for Counter DRBG; 444 and 888 bits for HMAC DRBG and Hash DRBG - 128-256 bits	SEED - CSP	Random Number Generation		Random Number Generation
Internal State (V, Key)	(compliant with IG D.L) Internal state of DRBG	256, 320, 384 bits for Counter DRBG; 320, 512, 1024 bits for HMAC DRBG - 128-256 bits	DRBG Internal state - CSP	Random Number Generation		Random Number Generation
Internal State (V, C)	(compliant with IG D.L) Internal state of DRBG	880, 1776 bits for Hash DRBG - 128-256 bits	DRBG Internal state - CSP	Random Number Generation		Random Number Generation
DH Public Key	Public key used for DH	2048, 3072, 4096, 6144, 8192 bits - 112-200 bits	Public key - PSP			Shared Secret Computation
DH Private Key	Private key used for DH	2048, 3072, 4096, 6144, 8192 bits - 112-200 bits	Private key - CSP			Shared Secret Computation
Module Generated DH Public Key	DH public key generated by the module	2048, 3072, 4096, 6144, 8192 bits - 112-200 bits	Public key - PSP	Key Pair Generation		
Module Generated DH Private Key	DH private key generated by the module	2048, 3072, 4096, 6144, 8192 bits - 112-200 bits	Private key - CSP	Key Pair Generation		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
EC Private Key	Private key used for ECDSA signature generation and Shared Secret Computation	P-224, P-256, P-384, P-521 - 128-256 bits	Private key - CSP			Shared Secret Computation
EC Public Key	Public key used for ECDSA signature verification primitive and Shared Secret Computation	P-224, P-256, P-384, P-521 - 128-256 bits	Public key - PSP			Shared Secret Computation
Module Generated EC Private Key	EC private key generated by the module	P-224, P-256, P-384, P-521 - 128-256 bits	Private key - CSP	Key Pair Generation		
Module Generated EC Public Key	EC public key generated by the module	P-224, P-256, P-384, P-521 - 128-256 bits	Public key - PSP	Key Pair Generation		
RSA Private Key	Private key used for RSA signature generation	2048, 3072, 4096 bits - 112, 128, 150 bits	Private key - CSP			Signature Generation
RSA Public Key	Public key used for RSA signature verification	1024, 2048, 3072, 4096 bits - 80, 112, 128, 150 bits	Public key - PSP			Signature Verification
Module Generated RSA Private Key	RSA private key generated by the module	2048, 3072, 4096 bits - 112, 128, 150 bits	Private key - CSP	Key Pair Generation		
Module Generated RSA Public Key	RSA public key generated by the module	2048, 3072, 4096 bits - 112, 128, 150 bits	Public key - PSP	Key Pair Generation		
TLS 1.2 Derived Secret	TLS derived secret	112-256 bits - 112-256 bits	Symmetric key - CSP	TLS v1.2 Key Derivation		
TLS 1.3 Derived Secret	TLS derived secret	112-256 bits - 112-256 bits	Symmetric key - CSP	TLS v1.3 Key Derivation		
Intermediate Key Generation Value	Intermediate key generation value	224-4096 bits - 112-256 bits	Intermediate value - CSP	Key Pair Generation		Key Pair Generation
HKDF Derived Key	HKDF derived key	112-2048 - 112-256 bits	Derived key - CSP	HKDF Key Derivation		
KBKDF Derived Key	Key-Based Derived Key	112-2048 - 112-256 bits	Derived Key - CSP	Key-Based Key Derivation		

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	
HMAC Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	
Shared Secret	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	DH Public Key:Generated From DH Private Key:Generated From EC Private Key:Generated From EC Public Key:Generated From Derived Key:Generated From
Password	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	PBKDF2 Derived Key:Derivation of
PBKDF2 Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Password:Derived From
KDA OneStep Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
KDA TwoStep Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
ANS X9.42 KDF Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
ANS X9.63 KDF Derived key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH KDF Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
Entropy Input		RAM:Plaintext	From generation until DRBG seed is created	Automatic	DRBG Seed:Generation of
DRBG Seed		RAM:Plaintext	While the DRBG is being instantiated	Automatic	Entropy Input:Derived From Internal State (V, Key):Generation of
Internal State (V, Key)		RAM:Plaintext	From DRBG instantiation until DRBG termination	Automatic	DRBG Seed:Generated From
Internal State (V, C)		RAM:Plaintext	From DRBG instantiation until DRBG termination	Automatic	DRBG Seed:Generated From
DH Public Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	DH Private Key:Paired With Shared Secret:Generation Of
DH Private Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	DH Public Key:Paired With Shared Secret:Generation Of
Module Generated DH Public Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated DH Private Key:Paired With Intermediate Key Generation Value:Generated From
Module Generated DH Private Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated DH Public Key:Paired With Intermediate Key Generation Value:Generated From
EC Private Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	EC Public Key:Paired With Shared Secret:Generation Of
EC Public Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	EC Private Key:Paired With Shared Secret:Generation Of

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Module Generated EC Private Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated EC Public Key:Paired With Intermediate Key Generation Value:Generated From
Module Generated EC Public Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated EC Private Key:Paired With Intermediate Key Generation Value:Generated From
RSA Private Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	RSA Public Key:Paired With
RSA Public Key	API input parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	RSA Private Key:Paired With
Module Generated RSA Private Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated RSA Public Key:Paired With Intermediate Key Generation Value:Generated From
Module Generated RSA Public Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Module Generated RSA Private Key:Paired With Intermediate Key Generation Value:Generated From
TLS 1.2 Derived Secret	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
TLS 1.3 Derived Secret	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API Remove power from the module	Shared Secret:Derived From
Intermediate Key Generation Value		RAM:Plaintext	For the duration of the service	Automatic	Module Generated DH Public Key:Generation Of Module Generated DH Private Key:Generation Of Module Generated EC Private Key:Generation Of Module Generated EC Public Key:Generation Of Module Generated RSA Private Key:Generation Of

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Module Generated RSA Public Key:Generation Of
HKDF Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API	Shared Secret:Derived From
KBKDF Derived Key	API output parameters	RAM:Plaintext	For the duration of the service	Calling the zeroization API	Shared Secret:Derived From

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.

The RSA, ECDSA algorithm as implemented by the module conforms to FIPS 186-4, which has been superseded by FIPS 186-5. FIPS 186-4 will be withdrawn on February 3, 2024.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A4317)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification
HMAC-SHA2-256 (A4318)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification
HMAC-SHA2-256 (A4326)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification
HMAC-SHA2-256 (A4330)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification
HMAC-SHA2-256 (A4344)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification
HMAC-SHA2-256 (A4346)	SHA2-256	HMAC	SW/FW Integrity	module inits	SHA2-256 HMAC verification

Table 21: Pre-Operational Self-Tests

The pre-operational software integrity test is performed automatically (after the CASTs) when the module is powered on before the module transitions into the operational state. The algorithm used for the integrity test (i.e., HMAC-SHA2-256) is self-tested before the software integrity test is performed. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module transitions to the operational state only after the pre-operational self-test has passed successfully. If the pre-operational self-test fails, the module transitions to the error state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A4316)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4321)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4322)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4323)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4335)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4336)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4337)	128-bit key, encrypt	KAT	CAST	Module becomes operational and	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use.		
AES-GCM (A4338)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4339)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4340)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4341)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4342)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-GCM (A4343)	128-bit key, encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
Counter DRBG (A4311)	128-bit key	KAT	CAST	Module becomes operational and services are available for use.	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4317)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4318)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4326)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4330)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4344)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A4345)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A4346)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4317)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4326)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4330)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4344)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4345)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A4346)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A4317)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A4326)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A4330)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A4344)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A4345)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A4346)	SHA2-512	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
RSA KeyGen (FIPS186-4) (A4317)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4326)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4330)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4344)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4345)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA KeyGen (FIPS186-4) (A4346)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA SigGen (FIPS186-4) (A4317)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4326)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4330)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4344)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4345)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-4) (A4346)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (A4317)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4326)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4330)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4344)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4345)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-4) (A4346)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA KeyGen (FIPS186-4) (A4317)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4326)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4330)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4344)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4345)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyGen (FIPS186-4) (A4346)	SHA2-256 and respective keys	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA SigGen (FIPS186-4) (A4312)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4317)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-4) (A4319)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4326)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4330)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4344)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4345)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-4) (A4346)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4312)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4317)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4319)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4326)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4330)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4344)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A4345)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A4346)	P-224 with SHA-224	KAT	CAST	Module becomes operational and services are available for use.	Digital signature verification	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4317)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4326)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4330)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4344)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4345)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A4346)	P-224 curve	KAT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A4325)	MODP-2048	PCT	CAST	Module becomes operational and services are available for use.	Shared secret computation	Test runs at power-on before the integrity test
AES-CBC (A4313)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A4314)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A4315)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A4327)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A4328)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A4329)	128-bit key encrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4313)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4314)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4315)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4320)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4327)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4328)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4329)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4331)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4332)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A4333)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A4334)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4313)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4314)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4315)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4327)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4328)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A4329)	128-bit key decrypt	KAT	CAST	Module becomes operational and services are available for use.	Symmetric operation	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A4317)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A4326)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A4330)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A4344)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512/256 (A4345)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A4346)	SHA2-512/256	KAT	CAST	Module becomes operational and services are available for use.	Message authentication	Test runs at power-on before the integrity test
KDF SP800-108 (A4324)	HMAC-SHA2-256 with 128-bit key, 24-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Key based key derivation	Test runs at power-on before the integrity test
KDA HKDF Sp800-56Cr1 (A4310)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Shared secret key derivation	Test runs at power-on before the integrity test
KDA OneStep SP800-56Cr2 (A4309)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use.	Shared secret key derivation	Test runs at power-on before the integrity test
KDA TwoStep SP800-56Cr2 (A4309)	SHA2-224	KAT	CAST	Module becomes operational and services are available for use.	Shared secret key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4312)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4317)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4319)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4326)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4330)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4344)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF ANS 9.42 (A4345)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.42 (A4346)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.42 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4312)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4317)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4319)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4326)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4330)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4344)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4345)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF ANS 9.63 (A4346)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based ANS X9.63 key derivation	Test runs at power-on before the integrity test
KDF SSH (A4320)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A4326)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH (A4331)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A4332)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A4333)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
KDF SSH (A4334)	SHA-1	KAT	CAST	Module becomes operational and services are available for use.	Industry-based SSH KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4317)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4326)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4330)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4344)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4345)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.2 KDF RFC7627 (A4346)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.2 KDF key derivation	Test runs at power-on before the integrity test
TLS v1.3 KDF (A4310)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Industry-based TLS v1.3 KDF key derivation	Test runs at power-on before the integrity test
PBKDF (A4312)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
PBKDF (A4317)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4319)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4326)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4330)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4344)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4345)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A4346)	SHA2-256 with 4096 iterations and 288-bit salt	KAT	CAST	Module becomes operational and services are available for use.	Password-based key derivation	Test runs at power-on before the integrity test
Hash DRBG (A4311)	HMAC-SHA-1, with PR	KAT	CAST	Module becomes operational and services are available for use.	Hash DRBG	Test runs at power-on before the integrity test
HMAC DRBG (A4311)	HMAC-SHA-1, with PR	KAT	CAST	Module becomes operational and services are available for use.	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Safe Primes Key Generation (A4325)	Section 5.6.2.1.4 of SP800-56Arev3	PCT	PCT	Module becomes operational and services are available for use.	SP 800-56ARev3, 5.6.2.1.4	Test runs at power-on before the integrity test
SHA-1 (A4317)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4326)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A4330)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4344)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4345)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA-1 (A4346)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4317)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4326)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4330)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4344)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4345)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A4346)	3-byte message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A4312)	32-bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test
SHA3-256 (A4319)	32-bit message	KAT	CAST	Module becomes operational and services are available for use.	Message digest	Test runs at power-on before the integrity test

Table 22: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A4317)	HMAC	SW/FW Integrity	on demand	module restart
HMAC-SHA2-256 (A4318)	HMAC	SW/FW Integrity	on demand	module restart
HMAC-SHA2-256 (A4326)	HMAC	SW/FW Integrity	on demand	module restart
HMAC-SHA2-256 (A4330)	HMAC	SW/FW Integrity	on demand	module restart
HMAC-SHA2-256 (A4344)	HMAC	SW/FW Integrity	on demand	module restart
HMAC-SHA2-256 (A4346)	HMAC	SW/FW Integrity	on demand	module restart

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A4316)	KAT	CAST	On Demand	Manually
AES-GCM (A4321)	KAT	CAST	On Demand	Manually
AES-GCM (A4322)	KAT	CAST	On Demand	Manually
AES-GCM (A4323)	KAT	CAST	On Demand	Manually
AES-GCM (A4335)	KAT	CAST	On Demand	Manually
AES-GCM (A4336)	KAT	CAST	On Demand	Manually
AES-GCM (A4337)	KAT	CAST	On Demand	Manually
AES-GCM (A4338)	KAT	CAST	On Demand	Manually
AES-GCM (A4339)	KAT	CAST	On Demand	Manually
AES-GCM (A4340)	KAT	CAST	On Demand	Manually
AES-GCM (A4341)	KAT	CAST	On Demand	Manually
AES-GCM (A4342)	KAT	CAST	On Demand	Manually
AES-GCM (A4343)	KAT	CAST	On Demand	Manually
Counter DRBG (A4311)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4317)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4318)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4326)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4330)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4344)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4345)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A4346)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4317)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A4326)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4330)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4344)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4345)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A4346)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4317)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4326)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4330)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4344)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4345)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A4346)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4317)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4326)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4330)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4344)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4345)	PCT	PCT	On Demand	Manually
RSA KeyGen (FIPS186-4) (A4346)	PCT	PCT	On Demand	Manually
RSA SigGen (FIPS186-4) (A4317)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4326)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4330)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4344)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4345)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4346)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4317)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4326)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4330)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4344)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A4345)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A4346)	KAT	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4317)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4326)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4330)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4344)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4345)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A4346)	PCT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4312)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4317)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4319)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4326)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4330)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4344)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4345)	KAT	CAST	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A4346)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4312)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4317)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4319)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4326)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4330)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4344)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4345)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A4346)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4317)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A4326)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4330)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4344)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4345)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4346)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A4325)	PCT	CAST	On Demand	Manually
AES-CBC (A4313)	KAT	CAST	On Demand	Manually
AES-CBC (A4314)	KAT	CAST	On Demand	Manually
AES-CBC (A4315)	KAT	CAST	On Demand	Manually
AES-CBC (A4327)	KAT	CAST	On Demand	Manually
AES-CBC (A4328)	KAT	CAST	On Demand	Manually
AES-CBC (A4329)	KAT	CAST	On Demand	Manually
AES-ECB (A4313)	KAT	CAST	On Demand	Manually
AES-ECB (A4314)	KAT	CAST	On Demand	Manually
AES-ECB (A4315)	KAT	CAST	On Demand	Manually
AES-ECB (A4320)	KAT	CAST	On Demand	Manually
AES-ECB (A4327)	KAT	CAST	On Demand	Manually
AES-ECB (A4328)	KAT	CAST	On Demand	Manually
AES-ECB (A4329)	KAT	CAST	On Demand	Manually
AES-ECB (A4331)	KAT	CAST	On Demand	Manually
AES-ECB (A4332)	KAT	CAST	On Demand	Manually
AES-ECB (A4333)	KAT	CAST	On Demand	Manually
AES-ECB (A4334)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4313)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4314)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4315)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4327)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4328)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A4329)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A4317)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A4326)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A4330)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A4344)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512/256 (A4345)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A4346)	KAT	CAST	On Demand	Manually
KDF SP800-108 (A4324)	KAT	CAST	On Demand	Manually
KDA HKDF Sp800-56Cr1 (A4310)	KAT	CAST	On Demand	Manually
KDA OneStep SP800-56Cr2 (A4309)	KAT	CAST	On Demand	Manually
KDA TwoStep SP800-56Cr2 (A4309)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4312)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4317)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4319)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4326)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4330)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4344)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4345)	KAT	CAST	On Demand	Manually
KDF ANS 9.42 (A4346)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4312)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4317)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4319)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4326)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4330)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4344)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4345)	KAT	CAST	On Demand	Manually
KDF ANS 9.63 (A4346)	KAT	CAST	On Demand	Manually
KDF SSH (A4320)	KAT	CAST	On Demand	Manually
KDF SSH (A4326)	KAT	CAST	On Demand	Manually
KDF SSH (A4331)	KAT	CAST	On Demand	Manually
KDF SSH (A4332)	KAT	CAST	On Demand	Manually
KDF SSH (A4333)	KAT	CAST	On Demand	Manually
KDF SSH (A4334)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4317)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4326)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4330)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4344)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4345)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A4346)	KAT	CAST	On Demand	Manually
TLS v1.3 KDF (A4310)	KAT	CAST	On Demand	Manually
PBKDF (A4312)	KAT	CAST	On Demand	Manually
PBKDF (A4317)	KAT	CAST	On Demand	Manually
PBKDF (A4319)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
PBKDF (A4326)	KAT	CAST	On Demand	Manually
PBKDF (A4330)	KAT	CAST	On Demand	Manually
PBKDF (A4344)	KAT	CAST	On Demand	Manually
PBKDF (A4345)	KAT	CAST	On Demand	Manually
PBKDF (A4346)	KAT	CAST	On Demand	Manually
Hash DRBG (A4311)	KAT	CAST	On Demand	Manually
HMAC DRBG (A4311)	KAT	CAST	On Demand	Manually
Safe Primes Key Generation (A4325)	PCT	PCT	On Demand	Manually
SHA-1 (A4317)	KAT	CAST	On Demand	Manually
SHA-1 (A4326)	KAT	CAST	On Demand	Manually
SHA-1 (A4330)	KAT	CAST	On Demand	Manually
SHA-1 (A4344)	KAT	CAST	On Demand	Manually
SHA-1 (A4345)	KAT	CAST	On Demand	Manually
SHA-1 (A4346)	KAT	CAST	On Demand	Manually
SHA2-512 (A4317)	KAT	CAST	On Demand	Manually
SHA2-512 (A4326)	KAT	CAST	On Demand	Manually
SHA2-512 (A4330)	KAT	CAST	On Demand	Manually
SHA2-512 (A4344)	KAT	CAST	On Demand	Manually
SHA2-512 (A4345)	KAT	CAST	On Demand	Manually
SHA2-512 (A4346)	KAT	CAST	On Demand	Manually
SHA3-256 (A4312)	KAT	CAST	On Demand	Manually
SHA3-256 (A4319)	KAT	CAST	On Demand	Manually

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module stops functioning and ends the Application process	When the Pre-Operational Self-Test or a CAST fails When a PCT fails Crypto operations requested in the Error state	The module must be restarted and successfully perform the pre-operational self-test and the CASTs to recover from these errors.	GNUTLS_E_SELF_TEST_ERROR (-400); GNUTLS_E_RANDOM_FAILED (-206); GNUTLS_E_PK_GENERATION_ERROR (-403); GNUTLS_E_LIB_IN_ERROR_STATE (-402)

Table 25: Error States

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

10.5 Operator Initiation of Self-Tests

The software integrity tests and CASTs can be invoked on demand by unloading and subsequently re-initializing the module. Additionally, the integrity test may be invoked on-demand by calling the OSSL_PROVIDER_self_test function. The PCTs can be invoked on demand by requesting the Key Pair Generation service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the Oracle Linux 9 (OL9) RPM package in the form of openssl-libs-3.0.7-24.0.3.el9_fips RPM package that is located in the "Oracle Linux 9 Security Validation (Update 3)" yum repository (ol9_u3_security_validation). Also, the module can be distributed using the openssl-fips-provider-3.0.7-6.0.1.el9_5 RPM package.

The module can achieve the approved mode by:

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

In both cases, the Crypto Officer must verify the Oracle Linux 9 system operates in approved mode by executing the fips-mode-setup –check command, which should output "FIPS mode is enabled."

For more information on Oracle Linux 9 system FIPS mode, please see Oracle Linux 9 product documentation.

After installation of the openssl-libs-3.0.7-24.0.3.el9_fips RPM package, the Crypto Officer must execute the openssl list -providers command. The Crypto Officer must ensure that the FIPS provider is listed in the output as follows:

fips
name: Oracle Linux 9 OpenSSL FIPS Provider
version: 3.0.7-b27cdeb3ba51be46
status: active

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

11.2 Administrator Guidance

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

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.4 End of Life

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory. Then, if desired, the openssl-libs-3.0.7-24.0.3.el9_fips RPM package can be uninstalled from the Oracle Linux 9 system.

12 Mitigation of Other Attacks

12.1 Attack List

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

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

In addition, RSA, ECDSA, ECDH, and DH employ blinding techniques to further impede timing and power analysis. No configuration is needed to enable the aforementioned countermeasures

Appendix A Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
CTS	Ciphertext Stealing
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Counter Mode Message Authentication Code
HKDF	HMAC-based Key Derivation Function
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
KBKDF	Key-based Key Derivation Function
KDA	Key Derivation Algorithm
KTS	Key Transport Scheme
KW	Key-Wrap
KWP	Key-Wrap with Padding
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PBKDF2	Password-based Key Derivation Function v2
PKCS	Public-Key Cryptography Standards
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
TOEPP	Tested Operational Environment's Physical Perimeter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B References

ANS X9.42-2001	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography 2001 https://webstore.ansi.org/standards/ascx9/ansix9422001
ANS X9.63-2001	Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography 2001 https://webstore.ansi.org/standards/ascx9/ansix9632001
FIPS 140-3	FIPS PUB 140-3 - Security Requirements For Cryptographic Modules March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS 140-3 IG	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	Secure Hash Standard (SHS) March 2012 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS 186-4	Digital Signature Standard (DSS) July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS 186-5	Digital Signature Standard (DSS) February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	Advanced Encryption Standard November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 https://www.ietf.org/rfc/rfc3447.txt
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) May 2003 https://www.ietf.org/rfc/rfc3526.txt
RFC 5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS August 2008 https://www.ietf.org/rfc/rfc5288.txt
RFC 7919	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS) August 2016 https://www.ietf.org/rfc/rfc7919.txt
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3 August 2018 https://www.ietf.org/rfc/rfc8446.txt

SP 800-38A	Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38A Addendum	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode October 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a-add.pdf
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC November 2007 https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices January 2010 https://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-52r2	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations August 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
SP 800-56Ar3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
SP 800-56Cr1	Recommendation for Key-Derivation Methods in Key-Establishment Schemes August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf
SP 800-56Cr2	Recommendation for Key-Derivation Methods in Key-Establishment Schemes August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf
SP 800-90Ar1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP 800-108r1	NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions August 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf
SP 800-131Ar2	Transitioning the Use of Cryptographic Algorithms and Key Lengths March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

SP 800-132	Recommendation for Password-Based Key Derivation - Part 1: Storage Applications December 2010 https://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
SP 800-133r2	Recommendation for Cryptographic Key Generation June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP 800-135r1	Recommendation for Existing Application-Specific Key Derivation Functions December 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SP 800-140B	CMVP Security Policy Requirements March 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf