Ctrl IQ, Inc.

Rocky Linux 8 and 9 libgcrypt Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

Document version: 1.1

Last update: 2025-12-18

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version rocky8.20240929 and rocky9.20240929 of the Rocky Linux 8 and 9 libgcrypt Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

This Security Policy describes the features and design of the module named Rocky Linux 8 and 9 libgcrypt Cryptographic Module using the terminology contained in the FIPS 140-3 specification. The FIPS 140-3 Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic module to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

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

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Rocky Linux 8 and 9 libgcrypt Cryptographic Module (hereafter referred to as "the module") is a software library implementing general purpose cryptographic algorithms. The module provides cryptographic services to applications running in the user space of the underlying operating system through an application program interface (API).

Module Type: Software

Module Embodiment: MultiChipStand

Cryptographic Boundary:

The module consists of the shared library file (i.e. libgcrypt.so.20) which constitutes the cryptographic boundary. The block diagram in Figure 1 shows the cryptographic boundary of the module, its interfaces with the operational environment and the flow of information between the module and operator. The block diagram is representative of both versions rocky8.20240929 and rocky9.20240929 of the cryptographic module.

Tested Operational Environment's Physical Perimeter (TOEPP):

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

The entropy source and the PAA provided by the processor are located within the module's physical perimeter and outside of the module's cryptographic boundary.

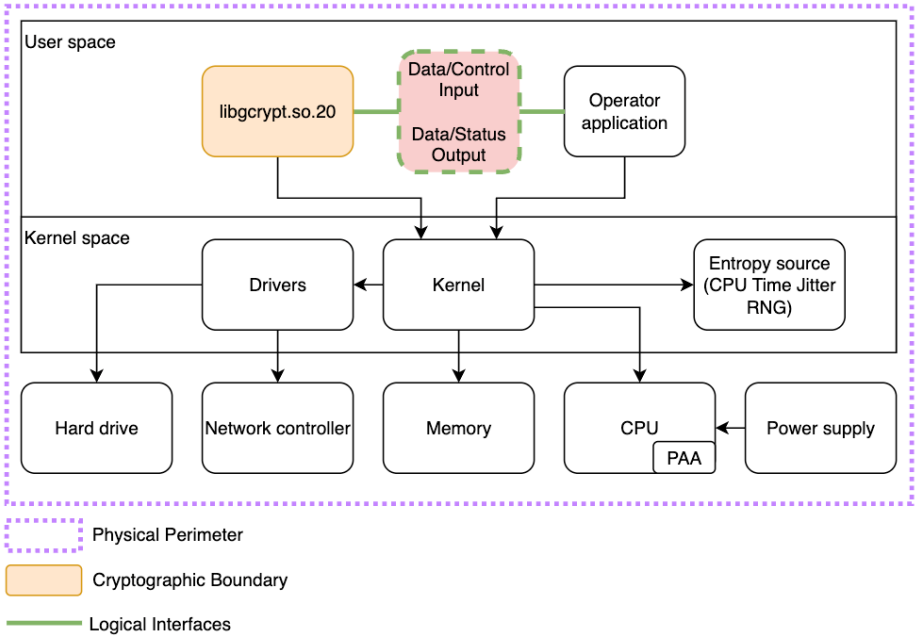

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:
N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
/usr/lib64/libgcrypt.so.20.5.0 on Rocky Linux 8	rocky8.20240929	N/A	HMAC-SHA-256
/usr/lib64/libgcrypt.so.20.5.0 on Rocky Linux 9	rocky9.20240929	N/A	HMAC-SHA-256

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

Tested Module Identification – Hybrid Disjoint Hardware:
N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Rocky Linux 8	SuperMicro SuperServer 5039MS	Intel Kaby Lake Xeon E3-1270 v6	Yes	N/A	rocky8.20240929
Rocky Linux 8	SuperMicro SuperServer 5039MS	Intel Kaby Lake Xeon E3-1270 v6	No	N/A	rocky8.20240929
Rocky Linux 9	SuperMicro SuperServer 5039MS	Intel Kaby Lake Xeon E3-1270 v6	Yes	N/A	rocky9.20240929
Rocky Linux 9	SuperMicro SuperServer 5039MS	Intel Kaby Lake Xeon E3-1270 v6	No	N/A	rocky9.20240929

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

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:
N/A for this module.

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service (the service API call return is GPG_ERR_NO_ERROR(0))
Non-approved Mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service (the service API call return is not GPG_ERR_NO_ERROR)

Table 4: Modes List and Description

Mode Change Instructions and Status:

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

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-KW	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Deterministic ECDSA SigGen (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
Hash DRBG	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
HMAC DRBG	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A6113, A6114, A6115, A6116, A6117, A6118, A6121, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/224	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-224	A6116, A6117, A6118, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6116, A6117, A6118, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6116, A6117, A6118, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6116, A6117, A6118, A6124, A6125, A6126	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
PBKDF	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Iteration Count - Iteration Count: 1000-10000000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Key Generation Mode - probable Modulo - 2048, 3072, 4096, 6144, 8192 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A6113, A6114, A6115, A6116, A6117, A6118, A6121, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-224	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-256	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-384	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA2-512/224	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512/256	A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 180-4
SHA3-224	A6116, A6117, A6118, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-256	A6116, A6117, A6118, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-384	A6116, A6117, A6118, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHA3-512	A6116, A6117, A6118, A6124, A6125, A6126	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1, 2, 4, 8	FIPS 202
SHAKE-128	A6116, A6117, A6118, A6124, A6125, A6126	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A6116, A6117, A6118, A6124, A6125, A6126	Output Length - Output Length: 16-65536 Increment 8	FIPS 202

Table 5: Approved Algorithms

The above table lists all approved cryptographic algorithms of the module, including specific key lengths employed for approved services, and implemented modes or methods of operation of the algorithms.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric Cryptographic Key Generation (CKG)	Key type:Asymmetric	N/A	SP 800-133 Rev.2 section 4, example 1

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:
N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:
N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
ECDH	Shared secret computation
AES-GCM, AES-GCM-SIV, AES-OCB, AES-EAX	Symmetric encryption; Symmetric decryption

Name	Use and Function
RSA	Signature generation (pre-hashed); Signature verification (pre-hashed); Asymmetric encryption (primitive); Asymmetric decryption (primitive)
ECDSA	Signature generation (pre-hashed); Signature verification (pre-hashed)

Table 7: Non-Approved, Not Allowed Algorithms

The table above lists all non-approved cryptographic algorithms of the module employed by the non-approved services.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Message digest with SHA-1	SHA	Message digest using SHA-1		SHA-1: (A6113, A6114, A6115, A6116, A6117, A6118, A6121, A6122, A6123, A6124, A6125, A6126)
Message digest with SHA-2	SHA	Message digest using SHA-2		SHA2-224: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) SHA2-256: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) SHA2-384: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) SHA2-512: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) SHA2-512/224: (A6114, A6115,

Name	Type	Description	Properties	Algorithms
				A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) SHA2-512/256: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Message digest with SHA-3	SHA XOF	Message digest using SHA-3		SHA3-224: (A6116, A6117, A6118, A6124, A6125, A6126) SHA3-256: (A6116, A6117, A6118, A6124, A6125, A6126) SHA3-384: (A6116, A6117, A6118, A6124, A6125, A6126) SHA3-512: (A6116, A6117, A6118, A6124, A6125, A6126) SHAKE-128: (A6116, A6117, A6118, A6124, A6125, A6126) SHAKE-256: (A6116, A6117, A6118, A6124, A6125, A6126)
Symmetric encryption	BC-UnAuth	Encryption using AES		AES-CBC: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-CFB128: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)

Name	Type	Description	Properties	Algorithms
				AES-CFB8: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-CTR: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-ECB: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-OFB: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Symmetric decryption	BC-UnAuth	Decryption using AES		AES-CBC: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-CFB128: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-CFB8: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-CTR: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-ECB: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)

Name	Type	Description	Properties	Algorithms
				AES-OFB: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Symmetric encryption with AES-XTS (for data storage)	BC-UnAuth	Encryption using AES-XTS (for data storage)		AES-XTS Testing Revision 2.0: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Symmetric decryption with AES-XTS (for data storage)	BC-UnAuth	Decryption using AES-XTS (for data storage)		AES-XTS Testing Revision 2.0: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Authenticated symmetric encryption	BC-Auth	Authenticated encryption using AES		AES-CCM: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-KW: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Authenticated symmetric decryption	BC-Auth	Authenticated decryption using AES		AES-CCM: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126) AES-KW: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Message authentication generation with AES-CMAC	MAC	Message authentication generation using AES-CMAC		AES-CMAC: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)

Name	Type	Description	Properties	Algorithms
Message authentication code with HMAC	MAC	Message authentication code using HMAC		HMAC-SHA-1: (A6113, A6114, A6115, A6116, A6117, A6118, A6121, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-224: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-256: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-384: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-512: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-512/224: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) HMAC-SHA2-512/256: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)

Name	Type	Description	Properties	Algorithms
				HMAC-SHA3-224: (A6116, A6117, A6118, A6124, A6125, A6126) HMAC-SHA3-256: (A6116, A6117, A6118, A6124, A6125, A6126) HMAC-SHA3-384: (A6116, A6117, A6118, A6124, A6125, A6126) HMAC-SHA3-512: (A6116, A6117, A6118, A6124, A6125, A6126)
Random number generation with CTR_DRBG	DRBG	Random number generation using CTR_DRBG		Counter DRBG: (A6114, A6115, A6117, A6118, A6122, A6123, A6125, A6126)
Random number generation with HMAC_DRBG	DRBG	Random number generation using HMAC_DRBG		HMAC DRBG: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Random number generation with Hash_DRBG	DRBG	Random number generation using Hash_DRBG		Hash DRBG: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Key pair generation with ECDSA	AsymKeyPair-KeyGen CKG	Key pair generation using ECDSA (IG D.H compliant)		ECDSA KeyGen (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) Asymmetric Cryptographic Key Generation (CKG): ()

Name	Type	Description	Properties	Algorithms
				Key type: Asymmetric
Public key verification with ECDSA	AsymKeyPair-KeyVer	Public key verification using ECDSA		ECDSA KeyVer (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Key pair generation with RSA	AsymKeyPair-KeyGen CKG	Key pair generation using RSA (IG D.H compliant)		RSA KeyGen (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126) Asymmetric Cryptographic Key Generation (CKG): () Key type: Asymmetric
Digital signature generation with ECDSA	DigSig-SigGen	Digital signature generation using ECDSA		ECDSA SigGen (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Deterministic digital signature generation with ECDSA	DigSig-SigGen	Deterministic digital signature generation using ECDSA		Deterministic ECDSA SigGen (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Digital signature generation with RSA	DigSig-SigGen	Digital signature generation using RSA		RSA SigGen (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)

Name	Type	Description	Properties	Algorithms
Digital signature verification with ECDSA	DigSig-SigVer	Digital signature verification using ECDSA		ECDSA SigVer (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Digital signature verification with RSA	DigSig-SigVer	Digital signature verification using RSA		RSA SigVer (FIPS186-5): (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)
Key derivation with PBKDF	PBKDF	Key derivation using PBKDF		PBKDF: (A6114, A6115, A6116, A6117, A6118, A6122, A6123, A6124, A6125, A6126)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES XTS

The length of a single data unit encrypted with the XTS-AES shall not exceed 2^{20} AES blocks, that is 16MB of data.

To meet the requirement stated in IG C.I, the module implements a check that ensures, before performing any cryptographic operation, that the two AES keys used in AES XTS mode are not identical.

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

Key_1 and Key_2 shall be generated and/or established independently according to the rules for component symmetric keys from NIST SP 800-133r2, Section 6.3.

Key derivation using SP800-132 PBKDF

The module provides password-based key derivation (PBKDF), compliant with SP800-132. The module supports option 1a from Section 5.4 of [SP800-132], in which the Master Key (MK) or a segment of it is used directly as the Data Protection Key (DPK).

In accordance with [SP800-132] and FIPS 140-3 IG D.N, the following requirements shall be met.

- Derived keys shall only be used in storage applications. The Master Key (MK) shall not be used for other purposes. The module accepts length of the MK or DPK of 112 bits or more.

- A portion of the salt, with a length of at least 128 bits, shall be generated randomly using the SP800-90A DRBG.
- 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 minimum value accepted by the module is 1000.
- Passwords or passphrases, used as an input for the PBKDF, shall not be used as cryptographic keys.
- The minimum length of the password or passphrase accepted by the module is 8 characters. The probability of guessing the value, assuming a worst-case scenario of all digits, 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.

The calling application shall also observe the rest of the requirements and recommendations specified in [SP800-132].

Authenticated encryption and 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.

SHA-1 Use

SHA-1 is only approved when used in approved modes for message digest and HMAC. The use of SHA-1 is non approved in any other case. Specifically, the use of SHA-1 for digital signature generation (e.g., ECSDA and RSA) or verification is non-approved.

2.8 RBG and Entropy

Cert Number	Vendor Name
E210	Ctrl IQ

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Rocky Linux Userspace CPU Time Jitter RNG Entropy Source	Non-Physical	Rocky Linux 8 on Intel Xeon E3-1270 v6; Rocky Linux 9 on Intel Xeon E3-1270 v6	256 bits	full entropy	SHA3-256

Table 10: Entropy Sources

The Module provides an SP800-90A-compliant Deterministic Random Bit Generator (DRBG) for creation of key components of asymmetric keys, and random number generation.

The seeding (and automatic reseeding) of the DRBG is done with get_random().

The module supports the Hash_DRBG, HMAC_DRBG and CTR_DRBG. The DRBG is initialized during module initialization; the module loads by default the DRBG using the HMAC_DRBG mechanism with SHA-256 and

without prediction resistance. A different DRBG mechanism can be chosen by invoking the gcry_control(GCRYCTL_DRBG_REINIT) function.

The module uses an [SP800-90B]-compliant entropy source specified in the above table. This entropy source is located within the module's physical perimeter but outside of the module's cryptographic boundary. The module obtains 384 bits to seed the DRBG and 256 bits to reseed it, respectively corresponding to 384 bits of entropy for seeding and 256 bits for reseeding, which is full entropy. Outputs of multiple GetEntropy() calls are concatenated to receive the entropy input length greater than 256 bits. The output is truncated to get the entropy input string which is not a multiple of 256.

The module performs the DRBG health tests as defined in Section 11.3 of [SP800-90A].

The module complies with the Public Use Document for ESV certificate E210 by reading entropy data from the get_random() function with the GRND_RANDOM flag set, which corresponds to the GetEntropy() conceptual interface. The operational environment on the ESV certificate is identical to the operating system described in this document. There are no maintenance requirements for the entropy source.

2.9 Key Generation

The module provides an [SP800-90Arev1]-compliant Deterministic Random Bit Generator (DRBG) for the creation of key components of asymmetric keys, and random number generation.

The Cryptographic Key Generation (CKG) methods implemented in the module for Approved services in approved mode are compliant with section 5.1 of [SP800-133rev2] and with IG D.H. For generating RSA and ECDSA keys the module implements asymmetric key generation services compliant with [FIPS186-5]. A seed (i.e., the random value) used in asymmetric key generation is directly obtained from the [SP800-90Arev1] DRBG.

Intermediate key generation values are not output from the module and are explicitly zeroized after processing the service.

2.10 Key Establishment

The module does not provide any key establisment mechanism.

2.11 Industry Protocols

The module does not implement industry protocols, therefore this section is not applicable.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 11: Ports and Interfaces

As a software-only module, the module does not have physical ports. The operator can only interact with the module through the API provided by the module. Thus, the physical ports are interpreted to be the physical ports of the hardware platform on which the module runs. The logical interfaces are logically separated from each other by the API design.

All data output via data output interface is inhibited when the module is performing pre-operational test or zeroization or when the module enters error state.

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

No support is provided for multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric encryption	Encrypt a plaintext	gcry_cipher_open returns GPG_ERR_NO_ERROR	AES key, plaintext	Ciphertext	Symmetric encryption Symmetric encryption with AES-XTS (for data storage)	Crypto Officer - AES key: W,E
Symmetric decryption	Decrypt a ciphertext	gcry_cipher_open returns GPG_ERR_NO_ERROR	AES key, ciphertext	Plaintext	Symmetric decryption Symmetric decryption with AES-XTS (for data storage)	Crypto Officer - AES key: W,E
Authenticated symmetric encryption	Encrypt and authenticate a plaintext	gcry_cipher_open returns GPG_ERR_NO_ERROR	AES key, plaintext, IV	Ciphertext, MAC tag	Authenticated symmetric encryption	Crypto Officer - AES key: W,E
Authenticated symmetric decryption	Decrypt and verify a ciphertext	gcry_cipher_open returns GPG_ERR_NO_ERROR	AES key, ciphertext, IV, MAC tag	Plaintext or fail	Authenticated symmetric decryption	Crypto Officer - AES key: W,E
Message digest	Compute SHA hashes	gcry_md_open returns GPG_ERR_NO_ERROR	Message	Digest value	Message digest with	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA-1 Message digest with SHA-2 Message digest with SHA-3	
Message authentication code (MAC) with HMAC	Compute HMAC	gcry_mac_open returns GPG_ERR_NO_ERROR	HMAC key, message	MAC tag	Message authentication code with HMAC	Crypto Officer - HMAC key: W,E
Message authentication code (MAC) with CMAC	Compute AES-based CMAC	gcry_mac_open returns GPG_ERR_NO_ERROR	AES key, message	MAC tag	Message authentication generation with AES-CMAC	Crypto Officer - AES key: W,E
Random Number Generation with CTR_DRBG	Generate random bitstrings from CTR_DRBG	gcry_randomize(), gcry_random_bytes(), gcry_random_bytes_secure() return GPG_ERR_NO_ERROR	Output length	Random bytes	Random number generation with CTR_DRBG	Crypto Officer - Entropy Input: W,E,Z - CTR_DRBG seed: G,E,Z - CTR_DRBG internal state (V value, Key): G,W,E
Random Number Generation with HMAC_DRBG	Generate random bitstrings from HMAC_DRBG	gcry_randomize(), gcry_random_bytes(), gcry_random_bytes_secure() return GPG_ERR_NO_ERROR	Output length	Random bytes	Random number generation with HMAC_DRBG	Crypto Officer - Entropy Input: W,E,Z - HMAC_DRBG seed: G,E,Z - HMAC_DR

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						BG internal state (V value, Key): G,W,E
Random Number Generation with Hash_DRBG	Generate random bitstrings from Hash_DRBG	gcry_randomize(), gcry_random_bytes(), gcry_random_bytes_secure() return GPG_ERR_NO_ERROR	Output length	Random bytes	Random number generation with Hash_DRBG	Crypto Officer - Entropy Input: W,E,Z - Hash_DRBG seed: G,E,Z - Hash_DRBG internal state (V value, C value): G,W,E
Key Pair Generation with RSA	Generate a key pair using RSA	gcry_pk_genkey returns GPG_ERR_NO_ERROR	Modulus bits	RSA public key, RSA private key	Random number generation with CTR_DRBG Random number generation with HMAC_DRBG Random number generation with Hash_DRBG Key pair generation with RSA	Crypto Officer - Module-generated RSA Private Key: G,R - Module-generated RSA Public Key: G,R - Intermediate key generation value: G,E,Z - Hash_DRBG internal state (V value, C value): W,E - HMAC_DR

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						BG internal state (V value, Key): W,E - CTR_DRBG internal state (V value, Key): W,E
Key Pair Generation with ECDSA	Generate a key pair using ECDSA	gcry_pk_genkey returns GPG_ERR_NO_ERROR	Curve	ECDSA public key, ECDSA private key	Random number generation with CTR_DRBG Random number generation with HMAC_DRBG Random number generation with Hash_DRBG Key pair generation with ECDSA	Crypto Officer - Module-generated ECDSA Private Key: G,R - Module-generated ECDSA Public Key: G,R - Intermediate key generation value: G,E,Z - Hash_DRBG internal state (V value, C value): W,E - HMAC_DRBG internal state (V value, Key): W,E - CTR_DRBG internal state (V

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						value, Key): W,E
Public key verification	Verify ECDSA public key	gcry_mpi_ec_curve_point() returns GPG_ERR_NO_ERROR	ECDSA public key	Pass/fail	Public key verification with ECDSA	Crypto Officer - ECDSA Public Key: W,E
Digital signature generation with RSA	Generate a signature using RSA	gcry_pk_hash_sign returns GPG_ERR_NO_ERROR	RSA private key, message	Signature	Random number generation with CTR_DRBG Random number generation with HMAC_DRBG Random number generation with Hash_DRBG Digital signature generation with RSA	Crypto Officer - RSA Private Key: W,E - Hash_DRBG internal state (V value, C value): W,E - HMAC_DRBG internal state (V value, Key): W,E - CTR_DRBG internal state (V value, Key): W,E
Digital signature generation with ECDSA	Generate a signature using ECDSA	gcry_pk_hash_sign returns GPG_ERR_NO_ERROR	ECDSA private key, message	Signature	Random number generation with CTR_DRBG Random number generation with HMAC_DRBG Random number	Crypto Officer - ECDSA Private Key: W,E - Hash_DRBG internal state (V value, C value): W,E - HMAC_DR

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					generation with Hash_DRBG Digital signature generation with ECDSA	BG internal state (V value, Key): W,E - CTR_DRBG internal state (V value, Key): W,E
Deterministic digital signature generation with ECDSA	Generate a signature using deterministic ECDSA	gcry_pk_hash_sign returns GPG_ERR_NO_ERROR	ECDSA private key, message	Signature	Deterministic digital signature generation with ECDSA	Crypto Officer - ECDSA Private Key: W,E
Digital signature verification with RSA	Verify a signature using RSA	gcry_pk_hash_verify returns GPG_ERR_NO_ERROR	RSA public key, message, signature	Pass/fail	Digital signature verification with RSA	Crypto Officer - RSA Public Key: W,E
Digital signature verification with ECDSA	Verify a signature using ECDSA	gcry_pk_hash_verify returns GPG_ERR_NO_ERROR	ECDSA public key, message, signature	Pass/fail	Digital signature verification with ECDSA	Crypto Officer - ECDSA Public Key: W,E
Key derivation	Perform key derivation	gcry_kdf_derive_fips returns GPG_ERR_NO_ERROR	Password, salt, iteration count, output length	Derived key	Key derivation with PBKDF	Crypto Officer - Password or passphrase: W,E - Derived key: G,R
On-demand Integrity test	Perform on-demand integrity test	N/A	N/A	Pass/fail	Message authentication code with HMAC	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show status	Show module status	N/A	N/A	Module status	None	Crypto Officer
Zeroization	Zeroize all SSPs	N/A	Any SSP	N/A	None	Crypto Officer
Self-tests	Perform self-tests	N/A	N/A	Pass/fail	None	Crypto Officer
Show module name and version	Show module name and version	N/A	N/A	Module name and version informati on	None	Crypto Officer

Table 13: Approved Services

The table above lists the approved services. For each service, the table lists the associated cryptographic algorithm(s), the role to perform the service, the cryptographic keys or CSPs involved, and their access type(s). The following convention is used to specify access rights to a CSP:

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

The details of the approved cryptographic algorithms including the CAVP certificate numbers can be found in the Approved Algorithm table.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Symmetric encryption	AES encryption using non-approved AES modes	AES-GCM, AES-GCM-SIV, AES-OCB, AES-EAX	CO
Symmetric decryption	AES decryption using non-approved AES modes	AES-GCM, AES-GCM-SIV, AES-OCB, AES-EAX	CO
Shared secret computation	ECDH Shared Secret Computation	ECDH	CO
Digital signature generation primitive	Generate a signature using ECDSA/RSA signature generation primitive	RSA ECDSA	CO
Digital signature verification primitive	Verify a signature using ECDSA/RSA signature verification primitive	RSA ECDSA	CO

Name	Description	Algorithms	Role
Asymmetric encryption primitive	Perform encryption using RSA encryption primitive	RSA	CO
Asymmetric decryption primitive	Perform decryption using RSA decryption primitive	RSA	CO

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

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

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified comparing the HMAC-SHA-256 value calculated at run time with the HMAC-SHA-256 value embedded in the module's ELF header that was computed at build time for each software component of the module. If the HMAC values do not match, the test fails and the module enters the error state.

5.2 Initiate on Demand

Integrity tests are performed as part of the Pre-Operational Self-Tests.

The module provides the Self-Test service to perform self-tests on demand which includes the pre-operational tests (i.e., integrity test) and cryptographic algorithm self-tests (CASTs). This service can be invoked relying on the gcry_control(GCRYCTL_SELFTEST) API function call or by powering-off and reloading the module. During the execution of the on-demand self-tests, services are not available, and no data output or input is possible.

In order to verify whether the self-tests have succeeded and the module is in the Operational state, the calling application may invoke the gcry_control(GCRYCTL_OPERATIONAL_P). The function will return TRUE if the module is in the operational state, FALSE if the module is in the Error state.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module operates in a modifiable operational environment per FIPS 140-3 level 1 specification: the module executes on a general-purpose operating system, which allows modification, loading, and execution of software that is not part of the validated module.

If properly installed, 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.

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 15: Storage Areas

SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls.

9.2 SSP Input-Output Methods

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

Table 16: SSP Input-Output Methods

The module does not support manual SSP entry or intermediate SSP generation output. The SSPs are provided to the module via API input parameters in plaintext form and output via API output parameters in plaintext form within the physical perimeter of the operational environment. This is allowed by [FIPS140-3_IG] 9.5.A, according to the "CM Software to/from App via TOEPP Path" entry on the Key Establishment Table.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the	By calling the cipher related zeroization API which are the following: gcry_free(), gcry_cipher_close(), gcry_mac_close(), gcry_sexp_release(), gcry_mpi_release(), gcry_ctx_release(), gcry_mpi_point_release(), gcry_ctrl(GCRYCTL_TERM_SECMEM)

Zeroization Method	Description	Rationale	Operator Initiation
		zeroization procedure succeeded.	
Automatic	Automatically zeroized by the module when no longer needed	Memory occupied by SSPs is overwritten with zeroes, which renders the SSP values irretrievable.	N/A
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module

Table 17: SSP Zeroization Methods

The memory occupied by SSPs is allocated by regular memory allocation operating system calls. The application that is acting as the CO is responsible for calling the appropriate zeroization functions provided in the module's API and listed in the above table. Calling gcry_free(), which will zeroize the SSPs and also invoke the corresponding API functions listed in the above table to zeroize SSPs. The zeroization functions overwrite the memory occupied by SSPs with “zeros” and deallocate the memory with the regular memory deallocation operating system call.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for encryption, decryption, and computing MAC tags	AES-XTS: 128, 256; Other modes: 128, 192, 256 - AES-XTS: 128, 256; Other modes: 128, 192, 256	Symmetric key - CSP			Symmetric encryption Symmetric decryption Authenticated symmetric encryption Authenticated symmetric decryption Symmetric encryption with AES-XTS (for data storage) Symmetric decryption with AES-XTS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						(for data storage) Message authentication generation with AES-CMAC
HMAC key	HMAC key used for computing MAC tags	112-524288 bits - 112-256 bits	Symmetric key - CSP			Message authentication code with HMAC
Module-generated RSA Private Key	RSA private key generated by the module	2048-8192 bits - 112-200 bits	Private key - CSP	Key pair generation with RSA		Key pair generation with RSA
Module-generated RSA Public Key	RSA public key generated by the module	2048-8192 bits - 112-200 bits	Public key - PSP	Key pair generation with RSA		Key pair generation with RSA
RSA Private Key	Private key used for RSA signature generation	2048-8192 bits - 112-200 bits	Private key - CSP			Digital signature generation with RSA
RSA Public Key	Public key used for RSA signature verification	2048-8192 bits bits - 112-200 bits	Public key - PSP			Digital signature verification with RSA
Module-generated ECDSA Private Key	ECDSA private key generated by the module	P-224, P-256, P-384, P-521 - 112, 128, 192, 256 bits	Private key - CSP	Key pair generation with ECDSA		Key pair generation with ECDSA
Module-generated ECDSA Public Key	ECDSA public key generated by the module	P-224, P-256, P-384, P-521 - 112, 128, 192, 256 bits	Public key - PSP	Key pair generation with ECDSA		Key pair generation with ECDSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDSA Private Key	Private key used for ECDSA signature generation and public key verification	P-224, P-256, P-384, P-521 - 112, 128, 192, 256 bits	Private key - CSP			Public key verification with ECDSA Digital signature generation with ECDSA Deterministic digital signature generation with ECDSA
ECDSA Public Key	Public key used for ECDSA signature verification	P-224, P-256, P-384, P-521 - 112, 128, 192, 256 bits	Public key - PSP			Digital signature verification with ECDSA
Intermediate key generation value	Intermediate key pair generation value generated during key generation and key derivation services (SP 800-133r2 Section 4, 5.1, and 5.2)	112-8192 - 112-256 bits	Intermediate value - CSP	Key pair generation with RSA Key pair generation with ECDSA		Key pair generation with RSA Key pair generation with ECDSA
Password or passphrase	Password used to derive symmetric keys	Minimum of 8 character - N/A	Password - CSP			Key derivation with PBKDF
Derived key	Symmetric key derived from a key derivation key, shared secret, or password	112-4096 bits - 112-256 bits	Symmetric key - CSP	Key derivation with PBKDF		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy Input	Entropy input used to seed the DRBG (IG D.L compliant)	128-384 bits - 128-384 bits	Entropy input - CSP			Random number generation with CTR_DRBG Random number generation with HMAC_DRBG Random number generation with Hash_DRBG
Hash_DRBG internal state (V value, C value)	Internal state of the Hash_DRBG (IG D.L compliant)	880, 1776 bits - 128, 256 bits	Internal state - CSP	Random number generation with Hash_DRBG		Random number generation with Hash_DRBG
CTR_DRBG internal state (V value, Key)	Internal state of the CTR_DRBG (IG D.L compliant)	256, 320, 384 bits - 128, 192, 256 bits	Internal state - CSP	Random number generation with CTR_DRBG		Random number generation with CTR_DRBG
HMAC_DRBG internal state (V value, Key)	Internal state of the HMAC_DRBG (IG D.L compliant)	320, 512, 1024 bits - 128, 256 bits	Internal state - CSP	Random number generation with HMAC_DRBG		Random number generation with HMAC_DRBG
Hash_DRBG seed	Hash_DRBG seed derived from entropy input as defined in SP 800-90Ar1 (IG D.L compliant)	440, 880 bits - 128, 256 bits;	Seed - CSP	Random number generation with Hash_DRBG		Random number generation with Hash_DRBG
CTR_DRBG seed	CTR_DRBG seed derived	256, 320, 384 bits -	Seed - CSP	Random number		Random number

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	from entropy input as defined in SP 800-90Ar1 (IG D.L compliant)	128, 192, 256 bits		generation with CTR_DRBG		generation with CTR_DRBG
HMAC_DRBG seed	HMAC_DRBG seed derived from entropy input as defined in SP 800-90Ar1 (IG D.L compliant)	440, 880 bits - 128, 256 bits	Seed - CSP	Random number generation with HMAC_DRBG		Random number generation with HMAC_DRBG

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	
HMAC key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	
Module-generated RSA Private Key	API output parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	Module-generated RSA Public Key:Paired With DRBG internal state (V value, Key):Generated from Intermediate key generation value:Generated from
Module-generated RSA Public Key	API output parameters (plaintext)	RAM:Plaintext	From service invocation until	Wipe and Free memory block	Module-generated RSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			cipherhandle is freed	allocated Module Reset	DRBG internal state (V value, Key):Generated from Intermediate key generation value:Generated from
RSA Private Key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	RSA Public Key:Paired With
RSA Public Key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	RSA Private Key:Paired With
Module-generated ECDSA Private Key	API output parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	Module-generated ECDSA Public Key:Paired With DRBG internal state (V value, Key):Generated from Intermediate key generation value:Generated from
Module-generated ECDSA Public Key	API output parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	Module-generated ECDSA Private Key:Paired With DRBG internal state (V value, Key):Generated from Intermediate key generation value:Generated from
ECDSA Private Key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	ECDSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ECDSA Public Key	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	ECDSA Private Key:Paired With
Intermediate key generation value		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	Module-generated RSA Private Key:Generates Module-generated RSA Public Key:Generates Module-generated ECDSA Private Key:Generates Module-generated ECDSA Public Key:Generates
Password or passphrase	API input parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	Derived key:Derivation of
Derived key	API output parameters (plaintext)	RAM:Plaintext	From service invocation until cipherhandle is freed	Wipe and Free memory block allocated Module Reset	Password or passphrase:Derived From
Entropy Input		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	DRBG seed:Derivation of
Hash_DRBG internal state (V value, C value)		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	DRBG seed:Generated from

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CTR_DRBG internal state (V value, Key)		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	DRBG seed:Generated from
HMAC_DRBG internal state (V value, Key)		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	DRBG seed:Generated from
Hash_DRBG seed		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	Entropy Input:Derived From Hash_DRBG internal state (V value, C value):Generation of
CTR_DRBG seed		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	Entropy Input:Derived From CTR_DRBG internal state (V value, Key):Generation of
HMAC_DRBG seed		RAM:Plaintext	From service invocation until cipherhandle is freed	Automatic	Entropy Input:Derived From HMAC_DRBG internal state (V value, Key):Generation of

Table 19: SSP Table 2

The tables above summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

9.5 Transitions

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A6114)	256-bit	Message authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for /usr/lib64/libgcrypt.so.20.5.0 on Rocky Linux 8
HMAC-SHA2-256 (A6122)	256-bit	Message authentication	SW/FW Integrity	Module becomes operational and services are available for use	Integrity test for /usr/lib64/libgcrypt.so.20.5.0 on Rocky Linux 9

Table 20: Pre-Operational Self-Tests

The module performs pre-operational self-tests automatically when the module is becoming available for the consuming application. Pre-operational self-tests ensure that the module is not corrupted. While the module is executing the pre-operational self-tests, services are not available, input and output are inhibited. The module is not available for use by the calling application until the pre-operational self-tests are completed successfully.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A6114)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6115)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6117)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6118)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Encrypt (A6122)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6123)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6125)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Encrypt (A6126)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6114)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6115)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6117)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6118)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6122)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6123)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB - Decrypt (A6125)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-ECB - Decrypt (A6126)	128, 192, 256-bit keys	KAT	CAST	Module becomes operational	Symmetric decrypt	Test runs at power-on before the integrity test
AES-CMAC (A6114)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6115)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6117)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6118)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6122)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6123)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6125)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
AES-CMAC (A6126)	128-bit key MAC generation	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A6114)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6115)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6117)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6118)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6122)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6123)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6125)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Counter DRBG (A6126)	AES 128-bit key with DF, with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6114)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6115)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A6116)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6117)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6118)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6122)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6123)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6124)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6125)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Hash DRBG (A6126)	SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6114)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6115)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A6116)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6117)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6118)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6122)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6123)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6124)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6125)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
HMAC DRBG (A6126)	HMAC-SHA2-256 with and without PR	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1 (seed, reseed, generate)	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6114)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6115)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Deterministic ECDSA SigGen (FIPS186-5) (A6116)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6117)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6118)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6122)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6123)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6124)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6125)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
Deterministic ECDSA SigGen (FIPS186-5) (A6126)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Deterministic digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6114)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6115)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	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 (FIPS186-5) (A6116)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6117)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6118)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6122)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6123)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6124)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6125)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigGen (FIPS186-5) (A6126)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6114)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6115)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A6116)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6117)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6118)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6122)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6123)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6124)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6125)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-5) (A6126)	P-256 and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6113)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6114)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A6115)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6116)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6117)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6118)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6121)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6122)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6123)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6124)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6125)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA-1 (A6126)	SHA-1	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A6114)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6115)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6116)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6117)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6118)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6122)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6123)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6124)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6125)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-224 (A6126)	SHA2-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A6114)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6115)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6116)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6117)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6118)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6122)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6123)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6124)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6125)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A6126)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A6114)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6115)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6116)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6117)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6118)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6122)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6123)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6124)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6125)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-384 (A6126)	SHA2-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A6114)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6115)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6116)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6117)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6118)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6122)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6123)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6124)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6125)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6126)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-224 (A6116)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6117)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6118)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6124)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6125)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6126)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A6116)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A6117)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A6118)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A6124)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-256 (A6125)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-256 (A6126)	SHA3-256	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6116)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6117)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6118)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6124)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6125)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-384 (A6126)	SHA3-384	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A6116)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A6117)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA3-512 (A6118)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A6124)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A6125)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
HMAC-SHA3-512 (A6126)	SHA3-512	KAT	CAST	Module becomes operational	Message authentication code	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6114)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6115)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6116)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6117)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6118)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6122)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	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 SigGen (FIPS186-5) (A6123)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6124)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6125)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigGen (FIPS186-5) (A6126)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6114)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6115)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6116)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6117)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6118)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6122)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-5) (A6123)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6124)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6125)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
RSA SigVer (FIPS186-5) (A6126)	PKCS#1 v1.5 with 2048-bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
SHA-1 (A6113)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6114)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6115)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6116)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6117)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6118)	SHA-1	KAT	CAST	Module becomes operational	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 (A6121)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6122)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6123)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6124)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6125)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA-1 (A6126)	SHA-1	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6114)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6115)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6116)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6117)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-224 (A6118)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6122)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6123)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6124)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6125)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-224 (A6126)	SHA2-224	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6114)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6115)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6116)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6117)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A6118)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6122)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6123)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6124)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6125)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-256 (A6126)	SHA2-256	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6114)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6115)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6116)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6117)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A6118)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6122)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6123)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6124)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6125)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-384 (A6126)	SHA2-384	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6114)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6115)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6116)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6117)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-512 (A6118)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6122)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6123)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6124)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6125)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
SHA2-512 (A6126)	SHA2-512	KAT	CAST	Module becomes operational	Message digest	Test runs at power-on before the integrity test
PBKDF (A6114)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6115)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	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 (A6116)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6117)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6118)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6122)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6123)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	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 (A6124)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6125)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
PBKDF (A6126)	SHA-1 password length 24 characters, master key length of 200 bits, iteration count of 4096, and salt length of 288 bits	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before the integrity test
RSA KeyGen (FIPS186-5) (A6114)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6115)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6116)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6117)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6118)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6122)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA KeyGen (FIPS186-5) (A6123)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6124)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6125)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
RSA KeyGen (FIPS186-5) (A6126)	PKCS#1 v1.5 with SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6114)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6115)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6116)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6117)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6118)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6122)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6123)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6124)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6125)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA KeyGen (FIPS186-5) (A6126)	SHA2-256	PCT	PCT	Key pair generation is successful	Signature generation and verification	Key pair generation

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6114)	Message authentication	SW/FW Integrity	On demand	Manually
HMAC-SHA2-256 (A6122)	Message authentication	SW/FW Integrity	On demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Encrypt (A6114)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6115)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6117)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6118)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6122)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6123)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6125)	KAT	CAST	On demand	Manually
AES-ECB - Encrypt (A6126)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6114)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6115)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6117)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6118)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB - Decrypt (A6122)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6123)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6125)	KAT	CAST	On demand	Manually
AES-ECB - Decrypt (A6126)	KAT	CAST	On demand	Manually
AES-CMAC (A6114)	KAT	CAST	On demand	Manually
AES-CMAC (A6115)	KAT	CAST	On demand	Manually
AES-CMAC (A6117)	KAT	CAST	On demand	Manually
AES-CMAC (A6118)	KAT	CAST	On demand	Manually
AES-CMAC (A6122)	KAT	CAST	On demand	Manually
AES-CMAC (A6123)	KAT	CAST	On demand	Manually
AES-CMAC (A6125)	KAT	CAST	On demand	Manually
AES-CMAC (A6126)	KAT	CAST	On demand	Manually
Counter DRBG (A6114)	KAT	CAST	On demand	Manually
Counter DRBG (A6115)	KAT	CAST	On demand	Manually
Counter DRBG (A6117)	KAT	CAST	On demand	Manually
Counter DRBG (A6118)	KAT	CAST	On demand	Manually
Counter DRBG (A6122)	KAT	CAST	On demand	Manually
Counter DRBG (A6123)	KAT	CAST	On demand	Manually
Counter DRBG (A6125)	KAT	CAST	On demand	Manually
Counter DRBG (A6126)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG (A6114)	KAT	CAST	On demand	Manually
Hash DRBG (A6115)	KAT	CAST	On demand	Manually
Hash DRBG (A6116)	KAT	CAST	On demand	Manually
Hash DRBG (A6117)	KAT	CAST	On demand	Manually
Hash DRBG (A6118)	KAT	CAST	On demand	Manually
Hash DRBG (A6122)	KAT	CAST	On demand	Manually
Hash DRBG (A6123)	KAT	CAST	On demand	Manually
Hash DRBG (A6124)	KAT	CAST	On demand	Manually
Hash DRBG (A6125)	KAT	CAST	On demand	Manually
Hash DRBG (A6126)	KAT	CAST	On demand	Manually
HMAC DRBG (A6114)	KAT	CAST	On demand	Manually
HMAC DRBG (A6115)	KAT	CAST	On demand	Manually
HMAC DRBG (A6116)	KAT	CAST	On demand	Manually
HMAC DRBG (A6117)	KAT	CAST	On demand	Manually
HMAC DRBG (A6118)	KAT	CAST	On demand	Manually
HMAC DRBG (A6122)	KAT	CAST	On demand	Manually
HMAC DRBG (A6123)	KAT	CAST	On demand	Manually
HMAC DRBG (A6124)	KAT	CAST	On demand	Manually
HMAC DRBG (A6125)	KAT	CAST	On demand	Manually
HMAC DRBG (A6126)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Deterministic ECDSA SigGen (FIPS186-5) (A6114)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6115)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6116)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6117)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6118)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6122)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6123)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6124)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6125)	KAT	CAST	On demand	Manually
Deterministic ECDSA SigGen (FIPS186-5) (A6126)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-5) (A6114)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6115)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6116)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6117)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6118)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6122)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6123)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6124)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6125)	KAT	CAST	On demand	Manually
ECDSA SigGen (FIPS186-5) (A6126)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6114)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6115)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6116)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A6117)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6118)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6122)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6123)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6124)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6125)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6113)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6114)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6115)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6121)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6122)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6123)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA-1 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6114)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6115)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6122)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6123)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA2-224 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6114)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6115)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6122)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6123)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6114)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6115)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6122)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6123)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA2-384 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6114)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6115)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6122)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6123)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-512 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA2-512 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA3-224 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA3-256 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA3-384 (A6125)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA3-384 (A6126)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6116)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6117)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6118)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6124)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6125)	KAT	CAST	On demand	Manually
HMAC-SHA3-512 (A6126)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6114)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6115)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6116)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6117)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6118)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6122)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6123)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6124)	KAT	CAST	On demand	Manually
RSA SigGen (FIPS186-5) (A6125)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-5) (A6126)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6114)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6115)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6116)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6117)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6118)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6122)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6123)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6124)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6125)	KAT	CAST	On demand	Manually
RSA SigVer (FIPS186-5) (A6126)	KAT	CAST	On demand	Manually
SHA-1 (A6113)	KAT	CAST	On demand	Manually
SHA-1 (A6114)	KAT	CAST	On demand	Manually
SHA-1 (A6115)	KAT	CAST	On demand	Manually
SHA-1 (A6116)	KAT	CAST	On demand	Manually
SHA-1 (A6117)	KAT	CAST	On demand	Manually
SHA-1 (A6118)	KAT	CAST	On demand	Manually
SHA-1 (A6121)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A6122)	KAT	CAST	On demand	Manually
SHA-1 (A6123)	KAT	CAST	On demand	Manually
SHA-1 (A6124)	KAT	CAST	On demand	Manually
SHA-1 (A6125)	KAT	CAST	On demand	Manually
SHA-1 (A6126)	KAT	CAST	On demand	Manually
SHA2-224 (A6114)	KAT	CAST	On demand	Manually
SHA2-224 (A6115)	KAT	CAST	On demand	Manually
SHA2-224 (A6116)	KAT	CAST	On demand	Manually
SHA2-224 (A6117)	KAT	CAST	On demand	Manually
SHA2-224 (A6118)	KAT	CAST	On demand	Manually
SHA2-224 (A6122)	KAT	CAST	On demand	Manually
SHA2-224 (A6123)	KAT	CAST	On demand	Manually
SHA2-224 (A6124)	KAT	CAST	On demand	Manually
SHA2-224 (A6125)	KAT	CAST	On demand	Manually
SHA2-224 (A6126)	KAT	CAST	On demand	Manually
SHA2-256 (A6114)	KAT	CAST	On demand	Manually
SHA2-256 (A6115)	KAT	CAST	On demand	Manually
SHA2-256 (A6116)	KAT	CAST	On demand	Manually
SHA2-256 (A6117)	KAT	CAST	On demand	Manually
SHA2-256 (A6118)	KAT	CAST	On demand	Manually
SHA2-256 (A6122)	KAT	CAST	On demand	Manually
SHA2-256 (A6123)	KAT	CAST	On demand	Manually
SHA2-256 (A6124)	KAT	CAST	On demand	Manually
SHA2-256 (A6125)	KAT	CAST	On demand	Manually
SHA2-256 (A6126)	KAT	CAST	On demand	Manually
SHA2-384 (A6114)	KAT	CAST	On demand	Manually
SHA2-384 (A6115)	KAT	CAST	On demand	Manually
SHA2-384 (A6116)	KAT	CAST	On demand	Manually
SHA2-384 (A6117)	KAT	CAST	On demand	Manually
SHA2-384 (A6118)	KAT	CAST	On demand	Manually
SHA2-384 (A6122)	KAT	CAST	On demand	Manually
SHA2-384 (A6123)	KAT	CAST	On demand	Manually
SHA2-384 (A6124)	KAT	CAST	On demand	Manually
SHA2-384 (A6125)	KAT	CAST	On demand	Manually
SHA2-384 (A6126)	KAT	CAST	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-512 (A6114)	KAT	CAST	On demand	Manually
SHA2-512 (A6115)	KAT	CAST	On demand	Manually
SHA2-512 (A6116)	KAT	CAST	On demand	Manually
SHA2-512 (A6117)	KAT	CAST	On demand	Manually
SHA2-512 (A6118)	KAT	CAST	On demand	Manually
SHA2-512 (A6122)	KAT	CAST	On demand	Manually
SHA2-512 (A6123)	KAT	CAST	On demand	Manually
SHA2-512 (A6124)	KAT	CAST	On demand	Manually
SHA2-512 (A6125)	KAT	CAST	On demand	Manually
SHA2-512 (A6126)	KAT	CAST	On demand	Manually
PBKDF (A6114)	KAT	CAST	On demand	Manually
PBKDF (A6115)	KAT	CAST	On demand	Manually
PBKDF (A6116)	KAT	CAST	On demand	Manually
PBKDF (A6117)	KAT	CAST	On demand	Manually
PBKDF (A6118)	KAT	CAST	On demand	Manually
PBKDF (A6122)	KAT	CAST	On demand	Manually
PBKDF (A6123)	KAT	CAST	On demand	Manually
PBKDF (A6124)	KAT	CAST	On demand	Manually
PBKDF (A6125)	KAT	CAST	On demand	Manually
PBKDF (A6126)	KAT	CAST	On demand	Manually
RSA KeyGen (FIPS186-5) (A6114)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6115)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6116)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6117)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6118)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6122)	PCT	PCT	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA KeyGen (FIPS186-5) (A6123)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6124)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6125)	PCT	PCT	On demand	Manually
RSA KeyGen (FIPS186-5) (A6126)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6114)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6115)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6116)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6117)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6118)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6122)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6123)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6124)	PCT	PCT	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A6125)	PCT	PCT	On demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) (A6126)	PCT	PCT	On demand	Manually

Table 23: Conditional Periodic Information

This information can be found in Section 5.2.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	The module will return an error code to indicate the error and will enter the Error state. Any further cryptographic operation is inhibited.	Failure of pre-operational tests or conditional tests.	The error can be recovered by a restart (i.e., powering off and powering on) of the module.	An error message related to the cause of the failure.
Fatal Error state	The module will abort and will not be available.	Random numbers are requested in the error state or cipher operations are requested on a deallocated handle.	The error can be recovered by a restart (i.e., powering off and powering on) of the module.	The module is aborted

Table 24: Error States

After the pre-operational self-tests and the CASTs succeed, the module becomes operational. If any of the pre-operational self-tests or any of the CASTs fail an error message is returned, and the module transitions to the error state.

The calling application can obtain the module state by calling the gcry_control(GCRYCTL_OPERATIONAL_P) API function. The function returns FALSE if the module is in the Error state, TRUE if the module is in the Operational state. In the Error state, all data output is inhibited, and no cryptographic operation is allowed.

10.5 Operator Initiation of Self-Tests

The software integrity tests and the CASTs can be invoked relying on the gcry_control(GCRYCTL_SELFTEST) API function call or by powering-off and reloading the module. The PCTs can be invoked on demand by requesting the Key Generation service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Crypto Officer can install the RPM package of the Module (i.e. libgcrypt-1.10.0-10.el8_6.ciqfips.0.4.rpm or libgcrypt-1.10.0-10.el9_2.ciqfips.0.4.rpm) using standard tools recommended for the installation of RPM packages on a Rocky Linux system (for example, dnf, rpm). The integrity of the RPM package is automatically verified during the installation, and the Crypto Officer shall not install the RPM package if there is any integrity error.

Before the RPM package of the module is installed, the system must operate in the FIPS-validated configuration. This can be achieved by:

- Starting the installation in the FIPS-validated configuration. 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 the FIPS-validated configuration after the installation. Execute the fips-mode-setup --enable command. Restart the system.

The Crypto Officer must verify the system operates in the FIPS-validated configuration by executing the fips-mode-setup --check command, which should output "FIPS mode is enabled." Note, this output confirms that the module is installed correctly in FIPS validated configuration and will operate as a FIPS validated module. It is not related to approved or non-approved mode of operation provided by the module, that is determined by the service indicator in section 2.4.

11.2 Administrator Guidance

After installation of the RPM package of the module, the operator needs to check the output of the gcry_get_config() API, which should include the following name and version:

Rocky Linux 8 Libgcrypt Cryptographic Module Version rocky8.20240929 (for Rocky Linux 8)

Rocky Linux 9 Libgcrypt Cryptographic Module Version rocky9.20240929 (for Rocky Linux 9)

Once libgcrypt has been put into the FIPS-validated configuration, it is not possible to switch back to standard mode without terminating the process first. If the logging verbosity level of libgcrypt has been set to at least 2, the state transitions and the self-tests are logged.

The user must not call malloc/free to create/release space for keys, let libgcrypt manage space for keys, which will ensure that the key memory is overwritten before it is released.

gcry_control(GCRYCTL_TERM_SECMEM) needs to be called before the process is terminated.

11.3 Non-Administrator Guidance

The module implements only the Crypto Officer. There are no requirements for non-administrator guidance.

11.4 End of Life

For secure sanitization of the cryptographic module, the module must first to be powered off, which will zeroize all keys and CSPs in volatile memory. Then, for actual deprecation, the module shall be upgraded to a newer version that is FIPS 140-3 validated.

The module does not possess persistent storage of SSPs, so further sanitization steps are not required.

12 Mitigation of Other Attacks

12.1 Attack List

RSA timing attacks.

12.2 Mitigation Effectiveness

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

By default, the module uses the following blinding technique: instead of using the RSA decryption directly, a blinded value $y = x\, r^e \ mod\ n$ is decrypted and the unblinded value $x' = y'\, r^{-1} \ mod\ n$ returned.

The blinding value r is a random value with the size of the modulus *n*.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
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
CKG	Cryptographic Key Generation
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DF	Derivation Function
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
KW	AES Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PAI	Processor Algorithm Implementation
PBKDF2	Password-based Key Derivation Function v2
PCT	Pair-wise Consistency Test
PKCS	Public-Key Cryptography Standards
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
XOF	Extendable Output Function
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS140-3_IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** October 2024 https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf
FIPS140-3_MM	**FIPS 140-3 Cryptographic Module Validation Program - Management Manual (Draft)** December 2022 https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/Draft%20FIPS-140-3-CMVP%20Management%20Manual%20v1.2%20%5BDec%2023%202022%5D.pdf
FIPS180-4	**Secure Hash Standard (SHS)** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-5	**Digital Signature Standard (DSS)** February 2023 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS197	**Advanced Encryption Standard** November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS202	**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
SP800-38A	**NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
SP800-38B	**NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf
SP800-38C	**NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP800-38E	**NIST Special Publication 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices** January 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

SP800-38F	**NIST Special Publication 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
SP800-90Arev1	**NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-90B	**NIST Special Publication 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
SP800-132	**NIST Special Publication 800-132 - Recommendation for Password-Based Key Derivation - Part 1: Storage Applications** December 2010 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
SP800-133rev2	**NIST Special Publication 800-133 - Recommendation for Cryptographic Key Generation** June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP800-140Br1	**NIST Special Publication 800-140B – Revision 1 - CMVP Security Policy Requirements** November 2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf