Apple Inc.

Apple corecrypto Module v13.0 [Intel, User, Software, SL1]

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
May 21st, 2026

Prepared by:

Lightship Security

Applus

www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Apple corecrypto Module v13.0 [Intel, User, Software, SL1], hereafter referred to as, “the module”. It contains the security rules under which the module must operate and describes how the module meets the requirements as specified in FIPS PUB 140-3 for an overall Security Level 1 cryptographic module.

1.2 Security Levels

The table below describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

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	N/A
	Overall Level	1

Table 1: Security Levels

The Module has an overall security level of 1.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module provides implementations of low-level cryptographic primitives to the Host OS's (macOS Ventura v13) Security Framework and Common Crypto. The module provides services intended to protect data in transit and at rest.

The module is optimized for library use within the Host OS user space and does not contain any terminating assertions or exceptions. It is implemented as a Host OS dynamically loadable library. After the library is loaded, its cryptographic functions are made available to the Host OS application.

Any internal error detected by the module is returned to the caller with an appropriate return code. The calling Host OS application must examine the return code and act accordingly. The module communicates any error status synchronously through the use of its documented return codes, thus indicating the module's status. Caller induced or internal errors do not reveal any sensitive material to callers.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the module is delineated by the dotted green rectangle, as shown in the figure below. The module executes within the user space of the computing platforms and operating systems listed in the Tested Operational Environments Table and Vendor-Affirmed Operational Environments Table.

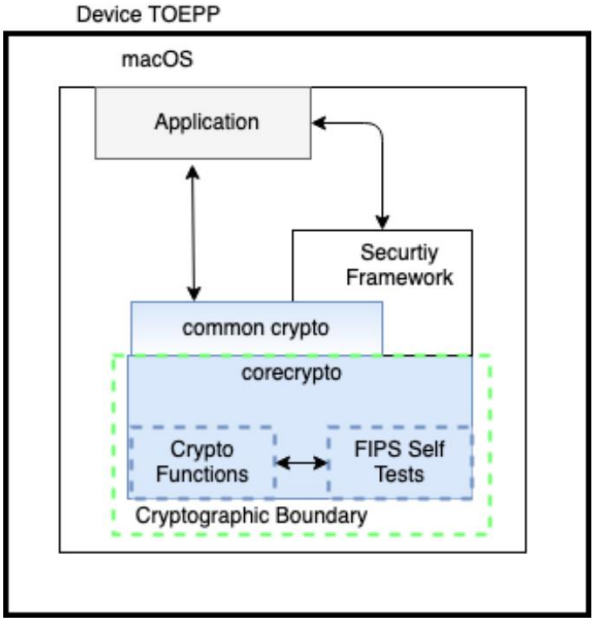

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical perimeter is represented by the most exterior black line in the block diagram (Figure 1).

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
corecrypto-1386.80.2	v13.0	N/A	HMAC-SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
macOS Ventura v13	MacBook Air 2022	Intel i5 (Amber Lake 8210Y)	Yes	N/A	v13.0
macOS Ventura v13	MacBook Air 2022	Intel i5 (Amber Lake 8210Y)	No	N/A	v13.0
macOS Ventura v13	MacBook Air 2022	Intel i7 (Ice Lake 1060NG7)	Yes	N/A	v13.0
macOS Ventura v13	MacBook Air 2022	Intel i7 (Ice Lake 1060NG7)	No	N/A	v13.0
macOS Ventura v13	MacBook Pro 2022	Intel i7 (Coffee Lake 8700B)	Yes	N/A	v13.0
macOS Ventura v13	MacBook Pro 2022	Intel i7 (Coffee Lake 8700B)	No	N/A	v13.0
macOS Ventura v13	iMac 2022	Intel i7 (Comet Lake 10700K)	Yes	N/A	v13.0
macOS Ventura v13	iMac 2022	Intel i7 (Comet Lake 10700K)	No	N/A	v13.0
macOS Ventura v13	MacBook Pro 2022	Intel i9 (Coffee Lake 9880H)	Yes	N/A	v13.0
macOS Ventura v13	MacBook Pro 2022	Intel i9 (Coffee Lake 9880H)	No	N/A	v13.0
macOS Ventura v13	iMac Pro 2022	Xeon W (SkyLake W-2140B)	Yes	N/A	v13.0
macOS Ventura v13	iMac Pro 2022	Xeon W (SkyLake W-2140B)	No	N/A	v13.0
macOS Ventura v13	Mac Pro 2022	Xeon W (Cascade Lake W-3223)	Yes	N/A	v13.0
macOS Ventura v13	Mac Pro 2022	Xeon W (Cascade Lake W-3223)	No	N/A	v13.0

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
macOS Ventura v13	Mac Pro 2022	Intel i5 (Coffee Lake 8257U)	Yes	N/A	v13.0
macOS Ventura v13	Mac Pro 2022	Intel i5 (Coffee Lake 8257U)	No	N/A	v13.0

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

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

Operating System	Hardware Platform
macOS Ventura v13	MacBook Pro - i5 (Ice Lake), 2021, 2020
macOS Ventura v13	MacBook Pro - i5 (Coffee Lake), 2021, 2020, 2019, 2018
macOS Ventura v13	MacBook Pro - i7 (Amber Lake), 2021, 2019, 2018
macOS Ventura v13	MacBook Pro - i7 (Coffee Lake), 2021, 2020, 2019, 2018
macOS Ventura v13	MacBook Pro - i7 (Ice Lake), 2021, 2020
macOS Ventura v13	MacBook Pro - i9 (Coffee Lake), 2021, 2019, 2018
macOS Ventura v13	MacBook Air - i5 (Ice Lake), 2021, 2020
macOS Ventura v13	MacBook Air - i7 (Ice Lake), 2021, 2020
macOS Ventura v13	MacBook Air - i5 (Amber Lake), 2021, 2019, 2018
macOS Ventura v13	MacBook Air - i7 (Amber Lake), 2021, 2018
macOS Ventura v13	Mac mini - i5 (Coffee Lake), 2021, 2018
macOS Ventura v13	Mac mini - i7 (Coffee Lake), 2021, 2018
macOS Ventura v13	iMac - i5 (Comet Lake), 2021, 2020
macOS Ventura v13	iMac - i7 (Comet Lake), 2021, 2020
macOS Ventura v13	iMac - i9 (Comet Lake), 2021, 2020
macOS Ventura v13	iMac - i5 (Coffee Lake), 2021, 2019
macOS Ventura v13	iMac - i7 (Coffee Lake), 2021, 2019
macOS Ventura v13	iMac - i9 (Coffee Lake), 2021, 2019
macOS Ventura v13	iMac - i9 (Comet Lake), 2022

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

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

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved mode	Approved mode of operation is entered when the module utilizes the services that use the security functions listed in the Approved Algorithms Table and the Vendor Affirmed Algorithms Table.	Approved	Return a '1' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was approved.
Non-Approved mode	Non-Approved mode of operation is entered when the module utilizes non-approved security functions in the Non-Approved Algorithms Not Allowed in the Approved Mode of Operation Table.	Non-Approved	Return a '0' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was non-approved.

Table 5: Modes List and Description

Mode Change Instructions and Status:

The Module has an Approved and Non-Approved mode of operation. The Approved mode of Operation is assumed automatically without any specific configuration. If the device starts up successfully then the module has passed all self-tests and is operating in the Approved mode. Any calls to the Non-Approved security functions listed in the Non-Approved Services Table will cause the module to assume the Non-Approved mode of operation.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3501	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3502	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3503	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C

Algorithm	CAVP Cert	Properties	Reference
AES-CCM	A3504	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CCM	A3509	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CCM	A3510	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CCM	A3511	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB128	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A3509	Direction - Generation, Verification Key Length - 128, 192, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-245760 Increment 8	SP 800-38B
AES-CTR	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3511	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A3501	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3502	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3511	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3503	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 8, 96, 1024	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 248	
AES-GCM	A3504	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 8, 96, 1024 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 248	SP 800-38D
AES-GCM	A3509	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 8, 96, 1024 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 248	SP 800-38D
AES-GCM	A3510	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 8, 96, 1024 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 248	SP 800-38D
AES-GCM	A3511	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 8, 96, 1024 Payload Length - Payload Length: 128, 256, 120, 248 AAD Length - AAD Length: 128, 256, 120, 248	SP 800-38D
AES-KW	A3503	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-KW	A3504	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 128-4096 Increment 128	
AES-KW	A3509	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-OFB	A3503	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A3504	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A3509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3501	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 65536 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A3502	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 65536 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A3503	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 65536 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A3504	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 65536 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A3509	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 65536 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
Counter DRBG	A3503	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256 Entropy Input - Entropy Input: 128, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64, 128 Personalization String Length - Personalization	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	
Counter DRBG	A3504	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256 Entropy Input - Entropy Input: 128, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64, 128 Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	SP 800-90A Rev. 1
Counter DRBG	A3509	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256 Entropy Input - Entropy Input: 128, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64, 128 Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	SP 800-90A Rev. 1
Counter DRBG	A3510	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256 Entropy Input - Entropy Input: 128, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64, 128 Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	SP 800-90A Rev. 1
Counter DRBG	A3511	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0, 128, Additional Input: 0, 256	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Entropy Input - Entropy Input: 128, Entropy Input: 256 Nonce - Nonce: 128, Nonce: 64, 128 Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	
ECDSA KeyGen (FIPS186-4)	A3505	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3506	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3507	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3509	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3505	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3506	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3507	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3509	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3505	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3506	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3507	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3509	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3505	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)	A3506	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3507	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3509	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC DRBG	A3505	Prediction Resistance - No Supports Reseed - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 128, 160, Entropy Input: 192, 256, Entropy Input: 256 Nonce - Nonce: 128, 256, Nonce: 64, 160, Nonce: 96, 256 Personalization String Length - Personalization String Length: 0, 160, Personalization String Length: 0, 256 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 384, 448, 640	SP 800-90A Rev. 1
HMAC DRBG	A3506	Prediction Resistance - No Supports Reseed - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 128, 160, Entropy Input: 192, 256, Entropy Input: 256 Nonce - Nonce: 128, 256, Nonce: 64, 160, Nonce: 96, 256 Personalization String Length - Personalization String Length: 0, 160, Personalization String Length: 0, 256 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 384, 448, 640	SP 800-90A Rev. 1
HMAC DRBG	A3507	Prediction Resistance - No Supports Reseed - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 128, 160, Entropy Input: 192, 256, Entropy Input: 256 Nonce - Nonce: 128, 256, Nonce: 64, 160, Nonce: 96, 256	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Personalization String Length - Personalization String Length: 0, 160, Personalization String Length: 0, 256 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 384, 448, 640	
HMAC DRBG	A3509	Prediction Resistance - No Supports Reseed - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Entropy Input - Entropy Input: 128, 160, Entropy Input: 192, 256, Entropy Input: 256 Nonce - Nonce: 128, 256, Nonce: 64, 160, Nonce: 96, 256 Personalization String Length - Personalization String Length: 0, 160, Personalization String Length: 0, 256 Additional Input - Additional Input: 0, 160, Additional Input: 0, 256 Returned Bits - 1024, 2048, 384, 448, 640	SP 800-90A Rev. 1
HMAC-SHA-1	A3505	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3506	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3507	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3509	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3512	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3505	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3506	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3507	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3509	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3512	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3505	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3506	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3507	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3509	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A3512	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3505	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3506	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3507	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3509	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3512	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3505	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3506	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3507	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3509	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3512	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3505	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3506	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3507	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3509	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3509	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC Component	A3509	Function - Full Public Key Validation Scheme - dhEphem - KAS Role - Initiator, Responder Shared Secret Computation - Parameter Set - FC - Hash Algorithm - SHA2-256	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3509	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Hash Function Z - SHA2-512	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		Scheme - dhEphem - KAS Role - initiator, responder	
KDF SP800-108	A3505	KDF Mode - Counter, Feedback MAC Mode - HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-4096 Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SP800-108	A3506	KDF Mode - Counter, Feedback MAC Mode - HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-4096 Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SP800-108	A3507	KDF Mode - Counter, Feedback MAC Mode - HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-4096 Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SP800-108	A3509	KDF Mode - Counter, Feedback MAC Mode - CMAC-AES128, CMAC-AES192, CMAC-AES256, HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-4096 Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 16, 24, 32, 8 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
PBKDF	A3505	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
PBKDF	A3506	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
PBKDF	A3507	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
PBKDF	A3509	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A3505	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A3506	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA KeyGen (FIPS186-4)	A3507	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A3509	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3505	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigGen (FIPS186-4)	A3506	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigGen (FIPS186-4)	A3507	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigGen (FIPS186-4)	A3509	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigVer (FIPS186-4)	A3505	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-4)	A3506	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-4)	A3507	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-4)	A3509	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
Safe Primes Key Generation	A3509	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-512	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3505	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3506	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3507	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3509	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
TDES-ECB	A3509	Direction - Decrypt, Encrypt Keying Option - 1	SP 800-67 Rev. 2

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	NIST SP800-133r2 Section 4: Using the Output of a Random Generator, Example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The table below lists all the Non-Approved, Allowed Algorithms with No Security Claimed.

Name	Caveat	Use and Function
MD5	Allowed in Approved mode with no security claimed per IG 2.4.A Digest Size: 128-bit	Message Digest (used as part of the TLS v1.0, v1.1 key establishment scheme only)

Table 8: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

The table below lists all the Non-Approved, Not Allowed Algorithms supported by the module.

Name	Use and Function
RSA Key Generation	ANSI X9.31 Key Pair Generation Key Size < 2048
RSA Digital Signature	PKCS#1 v1.5 and PSS; Signature Generation Key Size < 2048; Signature Verification Key Size < 1024
RSA Key Wrapping	OAEP, PKCS#1 v1.5 and PSS schemes
Diffie Hellman	Shared Secret Computation using key size < 2048
EC Diffie Hellman	Shared Secret Computation using curves < P-224

Name	Use and Function
X25519	Key Agreement, Key Generation
Ed25519	Key Generation, Signature Generation, Signature Verification
ANSI X9.63 KDF	Hash based Key Derivation Function
RFC6637	Key Derivation Function
HKDF [SP 800-56C]	Key Derivation Function
DES	Encryption/Decryption; Key Size: 56-bits
CAST5	Encryption/Decryption; Key Sizes: 40 to 128-bits in 8-bit increments
RC4	Encryption Decryption; Key Sizes: 8 to 4096-bits
RC2	Encryption/Decryption; Key Sizes 8 to 1024-bits
MD2	Message Digest; Digest size 128-bit
MD4	Message Digest, Digest size 128-bit
MD5	Message Digest size: 160-bit (except in the TLS 1.0/1.1 context)
RIPEMD	Message Digest; Digest size 160-bits
ECDSA	Key-pair generation: Curve P-192; Public key validation: Curve P-192; Signature Generation: Curve P-192; Signature Verification: Curve P-192; Key Pair Generation for compact point representation of points
Integrated Encryption Scheme on elliptic curves (ECIES)	Encryption/Decryption
Blowfish	Encryption/Decryption
OMAC (One-Key CBC MAC)	MAC generation
Triple-DES [SP 800-67r2]	CBC Encryption/Decryption and ECB encryption; Note: The module does not enforce the limit of 216 encryptions with the same Triple-DES key, as required by FIPS 140-3 IG C.G.

Table 9: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
AES Cipher	BC-UnAuth	AES Symmetric Encryption and Decryption		AES-CBC: (A3501, A3502, A3503, A3504, A3508, A3509) AES-CFB128: (A3503, A3504, A3509) AES-CFB8: (A3503, A3504, A3509) AES-CTR: (A3503, A3504, A3509, A3510, A3511) AES-ECB: (A3501, A3502,

Name	Type	Description	Properties	Algorithms
				A3503, A3504, A3509, A3510, A3511) AES-OFB: (A3503, A3504, A3509) AES-XTS Testing Revision 2.0: (A3501, A3502, A3503, A3504, A3509)
AES Authenticated Cipher	BC-Auth	AES Authenticated Encryption and Decryption		AES-CCM: (A3503, A3504, A3509, A3510, A3511) AES-GCM: (A3503, A3504, A3509, A3510, A3511) AES-KW: (A3503, A3504, A3509)
MAC (CMAC)	MAC	CMAC Generation and Verification		AES-CMAC: (A3509)
MAC (HMAC)	MAC	HMAC Generation and Verification		HMAC-SHA-1: (A3505, A3506, A3507, A3509, A3512) HMAC-SHA2-224: (A3505, A3506, A3507, A3509, A3512) HMAC-SHA2-256: (A3505, A3506, A3507, A3509, A3512) HMAC-SHA2-384: (A3505, A3506, A3507, A3509, A3512) HMAC-SHA2-512: (A3505, A3506, A3507, A3509, A3512) HMAC-SHA2-512/256: (A3505, A3506, A3507, A3509)

Name	Type	Description	Properties	Algorithms
Message Digest	SHA	SHA Digest and MD5 Digest		SHA-1: (A3505, A3506, A3507, A3509, A3512) SHA2-224: (A3505, A3506, A3507, A3509, A3512) SHA2-256: (A3505, A3506, A3507, A3509, A3512) SHA2-384: (A3505, A3506, A3507, A3509, A3512) SHA2-512: (A3505, A3506, A3507, A3509, A3512) SHA2-512/256: (A3505, A3506, A3507, A3509) MD5: ()
Key Derivation	KBKDF PBKDF	Key Derivation		KDF SP800-108: (A3505, A3506, A3507, A3509) PBKDF: (A3505, A3506, A3507, A3509)
Random Bit Generation	DRBG	Random Bit Generation		HMAC DRBG: (A3505, A3506, A3507, A3509) Counter DRBG: (A3503, A3504, A3509, A3510, A3511)
ECC Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer CKG	ECDSA Asymmetric Key Pair Generation and Verification		ECDSA KeyGen (FIPS186-4): (A3505, A3506, A3507, A3509) ECDSA KeyVer (FIPS186-4): (A3505, A3506, A3507, A3509) CKG: () Key Type: Asymmetric

Name	Type	Description	Properties	Algorithms
FFC Key Generation	AsymKeyPair-KeyGen CKG	Safe Primes Key Generation		Safe Primes Key Generation: (A3509) CKG: () Key Type: Asymmetric
IFC Key Generation	AsymKeyPair-KeyGen CKG	RSA Asymmetric Key Pair Generation		RSA KeyGen (FIPS186-4): (A3505, A3506, A3507, A3509) CKG: () Key Type: Asymmetric
ECDSA Digital Signature	DigSig-SigGen DigSig-SigVer	ECDSA Digital Signature Generation and Verification		ECDSA SigGen (FIPS186-4): (A3505, A3506, A3507, A3509) ECDSA SigVer (FIPS186-4): (A3505, A3506, A3507, A3509)
RSA Digital Signature	DigSig-SigGen DigSig-SigVer	RSA Digital Signature Generation and Verification		RSA SigGen (FIPS186-4): (A3505, A3506, A3507, A3509) RSA SigVer (FIPS186-4): (A3505, A3506, A3507, A3509)
ECC Key Agreement	KAS-SSC	ECC Key Agreement. Scheme: EphemeralUnified, KAS Role: Initiator, Responder	SP800-56Ar3 KAS-ECC-SSC per IG D.F Scenario 2 path (1):P-224, P-256, P-384, P-521 curves providing 112, 128, 192, or 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3509)
FFC Key Agreement	KAS-SSC	FFC Key Agreement. Scheme: dhEphem: KAS Role: initiator, responder	SP800-56Ar3 KAS-FFC-SSC IG D.F Scenario 2 path (1):2048, 3072, 4096, 6144, and 8192-bit key providing 112, 128, 152, 176, or 200 bits	KAS-FFC-SSC Sp800-56Ar3: (A3509) KAS-FFC Component: (A3509)

Name	Type	Description	Properties	Algorithms
			of security strength	
TDES Decryption	BC-UnAuthDecrypt	TDES Symmetric Decryption		TDES-ECB: (A3509)

Table 10: Security Function Implementations

MD5: Non-approved but allowed as part of the TLS key establishment scheme v1.0, v1.1 only with no security claimed.

2.7 Algorithm Specific Information

GCM IV

AES-GCM IV is constructed in compliance with IG C.H scenario 1 (TLS 1.2) and scenario 2 (IPsec-v3).

The GCM IV generation follows RFC 5288 shall only be used for the TLS protocol version 1.2. This implementation is compatible with acceptable AES-GCM cipher suites from SP800-52r2 Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the *nonce_explicit*, or counter portion of the IV will not exhaust all of its possible values.

The GCM IV generation follows RFC 4106 and shall only be used for the IPsec-v3 protocol version 3. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the IPsec protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the IPsec protocol implicitly ensures that the *nonce_explicit*, or counter portion of the IV will not exhaust all of its possible values.

In compliance with IG C.H section 3, if the module's power is lost and then restored, the key used for the AES GCM encryption/ decryption shall be re-distributed.

AES-XTS

AES-XTS mode is only approved for hardware storage applications. The length of the AES-XTS data unit does not exceed 2^{20} blocks. The module checks explicitly that Key_1 ≠ Key_2 before using the keys in the XTS-Algorithm to process data with them compliant with IG C.I.

Key Derivation using SP 800-132 PBKDF2

The module implements a CAVP tested key derivation function compliant to SP800-132 and IG D.N. The service returns the key derived from the provided password to the caller. The length of the password used as input to PBKDFv2 shall be at least 8 characters and the worst-case probability of guessing the value is 10^8 assuming all characters are digits only. The user shall choose the password length and the iteration count in such a way that the combination will make the key derivation computationally intensive. PBKDFv2 is implemented to support option 1a specified in section 5.4 of SP800-132.

Key Transport (KTS)

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.

Key Agreement (KAS)

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

2.8 RBG and Entropy

The tables below detail the modules ESV information.

Cert Number	Vendor Name
E14	apple
E110	apple

Table 11: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Apple corecrypto physical entropy source	Physical	See Tested Operational Environment Table in section 2.2	256 bits	256 bits	SHA2-256 [ACVP Cert. #C1223]
Apple corecrypto non-physical entropy source	Non-Physical	See Tested Operational Environment Table in section 2.2	256 bits	256 bits	SHA2-256 [ACVP Cert. #A3628]

Table 12: Entropy Sources

Entropy sources: Two entropy sources (one non-physical entropy source and one physical entropy source) residing within the TOEPP provide the random bits. The entropy sources are located within the physical perimeter of the module (TOEPP) but outside the cryptographic boundary of the module.

RBGs: The NIST SP 800-90ARev1 approved deterministic random bit generators (DRBG) used for random number generation is a CTR_DRBG using AES-256 with derivation function and without prediction resistance.

The module also employs a HMAC_DRBG for random number generation. The HMAC_DRBG is only used at the early boot time of macOS for memory randomization. The output of HMAC_DRBG is not used for key generation.

The module performs DRBG health tests according to SP800-90ARev1 section 11.3.

The deterministic random bit generators are seeded by /dev/random. The /dev/random is the User Space interface.

RBG Output: The output of entropy sources provides 256-bits of entropy to seed and reseed SP800-90ARev1 DRBG during initialization (seed) and reseeding (reseed).

2.9 Key Generation

The module generates Keys and SSPs in accordance with FIPS 140-3 IG D.H. The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP 800-133r2] Section 4, Example 1 (vendor affirmed), compliant with [FIPS186-4], and using DRBG compliant with [SP 800-90Ar1]. A seed (the random value) used in asymmetric key generation is obtained from [SP 800-90Ar1] DRBG. The key generation service for RSA, Diffie-Hellman and EC key pairs as well as the [SP 800-90Ar1] DRBG have been ACVT tested with algorithm certificates.

The module also implements the following key derivation functions:

- KBKDF Key Derivation according to [SP 800-108r1] to derive symmetric keys. The module supports Counter mode with AES-CMAC (128, 192, 256 bits), HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, or HMAC-SHA3-512 as the pseudo-random function (PRF).

- PBKDF Key Derivation according to [SP 800-132] to derive symmetric keys. The derived keys may only be used in storage applications. The module supports HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 as the pseudo-random function (PRF).

2.10 Key Establishment

The module provides the following SSP establishment related services in the Approved mode:

- Diffie-Hellman Shared Secret Computation

The module provides [SP 800-56Ar3] compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with DH shared secret computation. The shared secret computation provides between 112 and 200 bits of encryption strength.

- EC Diffie-Hellman Shared Secret Computation

The module provides [SP 800-56Ar3] compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with ECDH shared secret computation. The shared secret computation provides between 112 and 256 bits of encryption strength.

The module obtains the FIPS 140-3 IG D.F. Additional Comment 5 required key agreement assurances according to [SP 800-56Ar3] Section 5.6.2.

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The table below details the module Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	Data inputs are provided in the variables passed in the API and callable service invocations, generally through caller-supplied buffers.
N/A	Data Output	Data outputs are provided in the variables passed in the API and callable service invocations, generally through caller-supplied buffers.
N/A	Control Input	Control inputs which control the mode of the module are provided through dedicated parameters.
N/A	Status Output	Status output is provided in return codes and through messages. Documentation for each API lists possible return codes. A complete list of all return codes returned by the C language APIs within the module is provided in the header files and the API documentation. Messages are also documented in the API documentation.

Table 13: Ports and Interfaces

The module does not implement a Control Output Logical Interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

The module supports only one role that an operator may assume: Crypto Officer (CO) role. The CO role is assumed implicitly based on the service accessed. The Crypto Officer role is authorized to access all services provided by the module (see Table - Approved Services and Table - Non-Approved Services).

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 14: Roles

4.3 Approved Services

The table below lists all Approved Services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

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.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric encryption	Encrypt plaintext data	1	Plaintext data and key	Ciphertext data	AES Cipher AES Authenticated Cipher	Crypto Officer - AES key: W,E
Symmetric decryption	Decrypt ciphertext data	1	Ciphertext data and key	Plaintext data	AES Cipher AES Authenticated Cipher TDES Decryption	Crypto Officer - AES key: W,E - TDES Key: W,E
Key wrapping	Perform key wrapping	1	AES key wrapping key, key to be wrapped	Wrapped key	AES Authenticated Cipher	Crypto Officer - AES Key Wrapping key: W,E
Key unwrapping	Perform key unwrapping	1	Wrapped key, AES key wrapping key	Unwrapped key	AES Authenticated Cipher	Crypto Officer - AES Key Wrapping key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Hashing	Compute a message digest	1	Message	Digest	Message Digest	Crypto Officer
MAC Generation	Compute a message authentication code	1	Message, MAC key, MAC algorithm	MAC	MAC (CMAC) MAC (HMAC)	Crypto Officer - HMAC key: W,E - AES key: W,E
MAC Verification	Verify a message authentication code	1	MAC, message, MAC key, MAC algorithm	Pass/Fail	MAC (CMAC) MAC (HMAC)	Crypto Officer - AES key: W,E - HMAC key: W,E
Derive key via KBKDF	Derive key from key derivation key	1	KDF key derivation key	KDF derived key	Key Derivation	Crypto Officer - KBKDF Key derivation key: W,E - KBKDF Derived key: G,R
Derive Key via PBKDF	Derive key from password	1	Password	PBKDF derived key	Key Derivation	Crypto Officer - PBKDF Password: W,E - PBKDF derived key: G,R
ECDSA key pair generation	Generate a public/private key pair	1	Curve size	ECDSA key pair	ECC Key Generation	Crypto Officer - ECDSA private key: G,R - ECDSA public key: G,R
ECDSA signature generation	Sign a message with a specified ECDSA private key	1	Private key, message, hash function	Compute signature	ECDSA Digital Signature	Crypto Officer - ECDSA private key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
ECDSA signature verification	Verify the signature of a message with a specified ECDSA public key	1	Public key, digital signature, message, hash function	Pass/Fail result of digital signature verification	ECDSA Digital Signature	Crypto Officer - ECDSA public key: W,E
RSA key pair generation	Generate a public/private key pair	1	Key size	RSA Key pair	IFC Key Generation	Crypto Officer - RSA public key: G,R - RSA private key: G,R
RSA signature generation	Generate a digital signature	1	Private key, message, hash function	Computed signature	RSA Digital Signature	Crypto Officer - RSA private key: E
RSA signature verification	Verify a digital signature	1	Public key, digital signature, message, hash function	Pass/Fail result of digital signature verification	RSA Digital Signature	Crypto Officer - RSA public key: W,E
Safe primes key generation	Generate a keypair for a requested 'safe' domain parameter	1	Key size	FFC Key pair	FFC Key Generation	Crypto Officer - DH public key: G,R - DH private key: G,R
Diffie-Hellman Shared Secret Computation	Generate a shared secret	1	Domain parameter, received public key and possessed private key	Shared secret	FFC Key Agreement	Crypto Officer - DH public key: W,E - DH private key: E
EC Diffie-Hellman Shared Secret Computation	Generate a shared secret	1	Domain parameter, received public key and	Shared secret	ECC Key Agreement	Crypto Officer - EC DH public key: W,E - EC DH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			possessed private key			private key: E
Random number generation	Generate a random number	1	Requested number of bits	Random bit-string	Random Bit Generation	Crypto Officer - DRBG entropy input: W,E - DRBG Seed, Internal State V, and Key (IG D.L): G,E
Zeroisation	Zeroise all SSPs	1	Handler of crypto function context	Released memory space	None	Crypto Officer - AES key: Z - AES Key Wrapping key: Z - DH public key: Z - DH private key: Z - EC DH public key: Z - EC DH private key: Z - DRBG entropy input: Z - DRBG Seed, Internal State V, and Key (IG D.L): Z - ECDSA public key: Z - ECDSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						private key: Z - HMAC key: Z - KBKDF Key derivation key: Z - KBKDF Derived key: Z - RSA public key: Z - RSA private key: Z - PBKDF Password: Z - PBKDF derived key: Z - TDES Key: Z
On-Demand Self-test	Perform pre-operational and algorithm self-test	1	Instantiation	Status	AES Cipher AES Authenticated Cipher MAC (CMAC) MAC (HMAC) Message Digest Key Derivation Random Bit Generation ECC Key Generation FFC Key Generation IFC Key Generation ECDSA Digital Signature RSA Digital	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Signature ECC Key Agreement FFC Key Agreement TDES Decryption	
Show Status	Return module status	N/A	API invocation	Module status	None	Crypto Officer
Show Module and Version Information	Return module name and versioning information	N/A	API invocation	Module information	None	Crypto Officer

Table 15: Approved Services

4.4 Non-Approved Services

The table below lists all Non-Approved Services supported by the module.

Name	Description	Algorithms	Role
Triple-DES encryption/decryption	Module does not meet FIPS 140-3 IG C.G.; Input for Encryption: key and plain text; Output for Encryption: cipher text; Input for Decryption: key and ciphertext; Output for Decryption: plaintext	Triple-DES [SP 800-67r2]	CO
RSA Key Encapsulation	RSA encrypt/decrypt. Input (RSA encrypt): RSA public key, key to be wrapped; Output (RSA encrypt): wrapped key; Input (RSA decrypt): RSA private key, key to be unwrapped; Output (RSA encrypt): plaintext key	RSA Key Wrapping	CO
RSA Key-pair Generation	ANSI X9.31 Key-pair Generation; Key Size < 2048; Input: key size; Output: generated key pair	RSA Key Generation	CO
RSA Signature Generation	PKCS#1 v1.5 and PSS Signature Generation; Key Size < 2048; Input: RSA private key, message; Output: signature	RSA Digital Signature	CO
RSA Signature Verification	PKCS#1 v1.5 and PSS Signature Verification; Key Size < 1024; Input: RSA public key, signature; Output: true or false	RSA Digital Signature	CO
Diffie Hellman Shared Secret Computation	For key sizes < 2048; Input: peer public key and own private key; Output: shared secret	Diffie Hellman	CO
EC Diffie Hellman Shared Secret Computation	For curve sizes < P-224; Input: peer public key and own private key; Output: shared secret	EC Diffie Hellman	CO

Name	Description	Algorithms	Role
ECDSA Key-pair Generation (PKG) and ECDSA Key Validation (PKV)	ECDSA PKG and PKV using curve P-192; Input for PKG: curve size (P-192); Output: generated (P-192) private and public key pair; Input for PKV: public key; Output: True or False	ECDSA	CO
ECDSA Signature Generation	ECDSA Signature Generation using curve P-192; Input: (P-192) private key and message; Output: signature	ECDSA	CO
ECDSA Signature Verification	ECDSA Signature Verification using curve P-192; Input: (P-192) public key and signature; Output: True or False	ECDSA	CO
ECDSA Key Pair Generation for compact point representation of points	Key Pair Generation for compact point representation of points; Input: key size; Output: generated private and public key pair	ECDSA	CO
Ed25519/X25519 Key Generation	Ed25519 Key Generation; Input: none; Output: generated Ed25519/Curve25519 private and public key pair	X25519 Ed25519	CO
Ed25519 Signature Generation	Ed25519 Signature Generation over Curve25519; Input: (Ed25519) private key and message; Output: signature	Ed25519	CO
Ed25519 Signature Verification	EdDSA Signature Verification over Ed25519; Input: (Ed25519) public key and signature; Output: True or False	Ed25519	CO
X25519 Key Agreement	X25519 Key Agreement; Input: peer public key and own private key; Output: shared secret	X25519	CO
ECIES	Elliptic Curve encrypt/decrypt; Input for encryption: peer public key, plaintext; Output for encryption: public key, ciphertext (with authentication tag); Input for decryption: authentication tag, ciphertext, own private key; Output for decryption: plaintext message or error	Integrated Encryption Scheme on elliptic curves (ECIES)	CO
ANSI X9.63 Key Derivation	SHA-1 hash-based; Input: key derivation key; Output: derived key	ANSI X9.63 KDF	CO
SP 800-56C Key Derivation (HKDF)	SHA-256 hash-based; Input: key derivation key; Output: derived key	HKDF [SP 800-56C]	CO
RFC6637 Key Derivation	SHA hash based; Input: key derivation key; Output: derived key	RFC6637	CO
OMAC Message Authentication Code Generation and Verification	One-Key CBC-MAC using 128-bit key; For Message Authentication Code Generation: Input: message and key; Output: message authentication code (MAC); For Message Authentication Code Verification: Input: message, key, and MAC; Output: True or False	OMAC (One-Key CBC MAC)	CO

Name	Description	Algorithms	Role
Message digest generation	Message digest generation using non-approved algorithms; Input: message; Output: message digest	MD2 MD4 MD5 RIPEMD	CO
(other) symmetric encryption/decryption	Symmetric encryption/decryption using non-approved algorithms; Input for Encryption: key and plain text; Output for Encryption: cipher text; Input for Decryption: key and cipher text; Output for Decryption: plain text	DES CAST5 RC4 RC2 Blowfish	CO

Table 16: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support external software loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

A software integrity test is performed on the runtime image of the module. The HMAC-SHA2-256 implemented in the module is used as the approved algorithm for the integrity test. If the test fails, the module enters an error state where no cryptographic services are provided, and data output is prohibited i.e. the module is not operational.

5.2 Initiate on Demand

The module's integrity test can be performed on demand by self-test service or power-cycling the computing platform. Integrity test on demand is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

6.2 Configuration Settings and Restrictions

The module is supplied as part of macOS, a commercially available general-purpose operating system executing on the computing platforms specified in Section 2.2.

7 Physical Security

The FIPS 140-3 physical security requirements do not apply to the Apple corecrypto Module v13.0 [Intel, User, Software, SL1] since it is a software module.

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The table below lists Sensitive Security Parameters (SSPs) storage areas for the module. Section 9.4 below selects from the storage areas listed and specifies the appropriate parameter in the "Storage" column if applicable to a specific SSP.

Storage Area Name	Description	Persistence Type
RAM	The module stores ephemeral SSPs in RAM provided by the operational environment. They are received for use or generated by the module only at the command of the calling application. The operating system protects all SSPs through memory separation and protection mechanisms. No process other than the module itself can access the SSPs in its process' memory.	Dynamic

Table 17: Storage Areas

9.2 SSP Input-Output Methods

The table below lists SSP input and output methods for the module. Section 9.4 below selects from the input and output methods listed and specifies the appropriate parameter in the "Inputs/Outputs" column if applicable to a specific SSP.

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

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The table below lists SSP zeroisation methods for this module. Section 9.4 below selects from the zeroisation methods listed and specifies the appropriate parameter in the "Zeroization" column if applicable to a specific SSP.

Zeroization Method	Description	Rationale	Operator Initiation
Context object destruction	SSPs are zeroised when the appropriate context object is destroyed.	Zeroization when structure is deallocated.	Invocation of zeroization function cc_clear().
Power down	SSPs are zeroised when the system is powered down.	SSPs are zeroised when the system is powered down.	Operator can initiate power down.

Zeroization Method	Description	Rationale	Operator Initiation
Intermediate value zeroization	Intermediate keygen values are zeroized before the module returns from the key generation function.	Intermediate keygen values are zeroized before the module returns from the key generation function.	N/A

Table 19: SSP Zeroization Methods

9.4 SSPs

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Cipher AES Authenticated Cipher MAC (CMAC)
AES Key Wrapping key	AES-KW key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Authenticated Cipher
DH public key	Diffie-Hellman public key (including intermediate keygen values)	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits	Asymmetric Key - PSP	FFC Key Generation		FFC Key Agreement
DH private key	Diffie-Hellman private key (including intermediate keygen values)	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits	Asymmetric Key - CSP	FFC Key Generation		FFC Key Agreement

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
EC DH public key	EC Diffie-Hellman public key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - PSP	ECC Key Generation		ECC Key Agreement
EC DH private key	EC Diffie-Hellman private key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - CSP	ECC Key Generation		ECC Key Agreement
DRBG entropy input	Entropy input string	256 bits - 256 bits	Entropy input string - CSP			Random Bit Generation
DRBG Seed, Internal State V, and Key (IG D.L)	DRBG input parameters	256 bits - 256 bits	DRBG parameters - CSP	Random Bit Generation		Random Bit Generation
ECDSA public key	ECDSA public key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - PSP	ECC Key Generation		ECDSA Digital Signature
ECDSA private key	ECDSA private key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - CSP	ECC Key Generation		ECDSA Digital Signature
HMAC key	HMAC key	>=112 bits - >=112 bits	MAC Key - CSP			MAC (HMAC)
KBKDF Key derivation key	KBKDF key derivation key	Min: 112 bits - Min: 112 bits	Derivation Key - CSP			Key Derivation
KBKDF Derived key	KBKDF derived key	Min: 112 bits - Min: 112 bits	Derived Key - CSP	Key Derivation		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA public key	RSA public key (including intermediate keygen values)	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - PSP	IFC Key Generation		RSA Digital Signature
RSA private key	RSA private key (including intermediate keygen values)	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - CSP	IFC Key Generation		RSA Digital Signature
PBKDF Password	PBKDF input password	64 to 1024 bits - N/A	Password - CSP			Key Derivation
PBKDF derived key	PBKDF derived key	Min: 112 bits - Min: 112 bits	Derived Key - CSP	Key Derivation		
TDES Key	TDES key	168 bits - 112 bits	Symmetric Key - CSP			TDES Decryption

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	
AES Key Wrapping key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	
DH public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	DH private key:Paired With
DH private key	API output parameters	RAM:Plaintext	From service invocation	Context object destruction Power down	DH public key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			to service completion	Intermediate value zeroization	
EC DH public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	EC DH private key:Paired With
EC DH private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	EC DH public key:Paired With
DRBG entropy input	API input parameters	RAM:Plaintext	From service invocation to service completion	Power down	DRBG Seed, Internal State V, and Key (IG D.L):Generates
DRBG Seed, Internal State V, and Key (IG D.L)		RAM:Plaintext	From service invocation to service completion	Power down	DRBG entropy input:Generated From
ECDSA public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	ECDSA private key:Paired With
ECDSA private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	ECDSA public key:Paired With
HMAC key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KBKDF Key derivation key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KBKDF Derived key:Derives
KBKDF Derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KBKDF Key derivation key:Derived From
RSA public key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	RSA private key:Paired With
RSA private key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	RSA public key:Paired With
PBKDF Password	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF derived key:Derives
PBKDF derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF Password:Derived From
TDES Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	

Table 21: SSP Table 2

10 Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module. The pre-operational and conditional self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

10.1 Pre-Operational Self-Tests

Pre-operational Self-Tests are run upon the power up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests are passed successfully. The design of the module ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition. The Pre-Operational Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A3512)	112-bit key	Message Authentication over the complete module file image	SW/FW Integrity	Module successful execution	The HMAC-SHA2-256 value calculated at runtime is compared with the HMAC-SHA2-256 value stored in the module, computed at compilation time

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Conditional Self-Tests are run when an applicable security function or process is invoked. The Conditional Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A3505)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A3506)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A3507)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A3509)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A3512)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on before the integrity test
AES-CBC (A3501)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3502)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3508)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
AES-CCM (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3510)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3511)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes	Authenticated Encryption/Decryption	Test runs at power-on after

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				operational		the integrity test
AES-GCM (A3510)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3511)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A3501)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A3502)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3501)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3502)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3510)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3511)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-KW (A3503)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
AES-KW (A3504)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-KW (A3509)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
Counter DRBG (A3503)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
Counter DRBG (A3504)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
Counter DRBG (A3509)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
Counter DRBG (A3510)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
Counter DRBG (A3511)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
HMAC DRBG (A3505)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes	Compliant with SP 800-90Ar1	Test runs at power-on after

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				operational		the integrity test
HMAC DRBG (A3506)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
HMAC DRBG (A3507)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
HMAC DRBG (A3509)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3505)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3506)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3507)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3509)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 (A3512)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3505)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3506)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3507)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3509)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3512)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
AES-CMAC (A3509)	128-bit key	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3505)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
RSA SigGen (FIPS186-4) (A3506)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3507)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3509)	PKCS#1v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-4) (A3505)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-4) (A3506)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-4) (A3507)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-4) (A3509)	2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-	P-256 curve with SHA2-256	KAT	CAST	Module becomes	Digital Signature Generation	Test runs at power-on after

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
4) (A3505)				operational		the integrity test
ECDSA SigGen (FIPS186-4) (A3506)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A3507)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A3509)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3505)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3506)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3507)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3509)	P-256 curve with SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-FFC-SSC Sp800-56Ar3 (A3509)	Diffie-Hellman "Z" computation	KAT	CAST	Module becomes operational	DH Shared Secret Computation	Test runs at power-on after the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A3509)	EC Diffie-Hellman "Z" computation	KAT	CAST	Module becomes operational	ECDH Shared Secret Computation	Test runs at power-on after the integrity test
PBKDF (A3505)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A3506)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A3507)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A3509)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
KDF SP800-108 (A3505)	Counter and Feedback modes	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
KDF SP800-108 (A3506)	Counter and Feedback modes	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
KDF SP800-108 (A3507)	Counter and Feedback modes	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
KDF SP800-108 (A3509)	Counter and Feedback modes	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
TDES-ECB (A3509)	168-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
ECDSA KeyGen (FIPS186-4) (A3505)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3506)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3507)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3509)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
Safe Primes Key Generation (A3509)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen	PCT	PCT	PCT	Successful key pair	Key Generation	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-4) (A3505)				generation		
RSA KeyGen (FIPS186-4) (A3506)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A3507)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A3509)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

Table 23: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms supported in the approved mode of operation, using the tests shown in the table above. To ensure all conditional CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module's initial power-up sequence. The CASTs for algorithms used in the pre-operational software integrity test are performed prior to the integrity test itself; all other CASTs are executed immediately after the successful completion of the software integrity test.

Services are not available, and data output (via the data output interface) is inhibited during the self-tests. If any of these tests fail, the module transitions to the error state.

10.3 Periodic Self-Test Information

Pre-operational self-tests can be run on-demand, for periodic testing, by self-test service or rebooting the module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3512)	Message Authentication over the complete module file image	SW/FW Integrity	Whenever module is powered on	Upon every power on

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3505)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3506)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3507)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3509)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3512)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3501)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3502)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3503)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3504)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3508)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3509)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3503)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3504)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3509)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3510)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3511)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3503)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3504)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3509)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3510)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3511)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3501)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3502)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A3503)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3504)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3509)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3501)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3502)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3503)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3504)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3509)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3510)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3511)	KAT	CAST	On Demand	Power cycle
AES-KW (A3503)	KAT	CAST	On Demand	Power cycle
AES-KW (A3504)	KAT	CAST	On Demand	Power cycle
AES-KW (A3509)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3503)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3504)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3509)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3510)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3511)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3505)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3506)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3507)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3509)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A3505)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3506)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3507)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3509)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3512)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3505)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3506)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3507)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3509)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3512)	KAT	CAST	On Demand	Power cycle
AES-CMAC (A3509)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3505)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3506)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3507)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3509)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3505)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3506)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3507)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3509)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-4) (A3505)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3506)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3507)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3509)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3505)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3506)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3507)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3509)	KAT	CAST	On Demand	Power cycle
KAS-FFC-SSC Sp800-56Ar3 (A3509)	KAT	CAST	On Demand	Power cycle
KAS-ECC-SSC Sp800-56Ar3 (A3509)	KAT	CAST	On Demand	Power cycle
PBKDF (A3505)	KAT	CAST	On Demand	Power cycle
PBKDF (A3506)	KAT	CAST	On Demand	Power cycle
PBKDF (A3507)	KAT	CAST	On Demand	Power cycle
PBKDF (A3509)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3505)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3506)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3507)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3509)	KAT	CAST	On Demand	Power cycle
TDES-ECB (A3509)	KAT	CAST	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A3505)	PCT	PCT	On Demand	On generating keys for ECC

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-4) (A3506)	PCT	PCT	On Demand	On generating keys for ECC
ECDSA KeyGen (FIPS186-4) (A3507)	PCT	PCT	On Demand	On generating keys for ECC
ECDSA KeyGen (FIPS186-4) (A3509)	PCT	PCT	On Demand	On generating keys for ECC
Safe Primes Key Generation (A3509)	PCT	PCT	On Demand	On generating keys for DH
RSA KeyGen (FIPS186-4) (A3505)	PCT	PCT	On Demand	On generating keys for RSA
RSA KeyGen (FIPS186-4) (A3506)	PCT	PCT	On Demand	On generating keys for RSA
RSA KeyGen (FIPS186-4) (A3507)	PCT	PCT	On Demand	On generating keys for RSA
RSA KeyGen (FIPS186-4) (A3509)	PCT	PCT	On Demand	On generating keys for RSA

Table 25: Conditional Periodic Information

10.4 Error States

The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
Error State	1) The HMAC-SHA2-256 value computed over the module did not match the precomputed value or 2) The computed value in the invoked Conditional CAST did	1) Preoperational Software Integrity Test failure 2) Conditional CAST failure 3) Conditional PCT failure	Power cycle the device which results in the module being reloaded into memory and reperforming the preoperational software integrity test and the Conditional CASTs	1) Error message "FAILED: fipspost_post_integrity" send to caller or 2) Error message "FAILED:<event>" sent to caller (<event> refers to any of the cryptographic functions listed Table - Conditional Self-Tests, 3) Error code "CCEC_GENERATE_KEY_CONSISTENCY" returned for ECDSA and EC Diffie- Hellman Error code "CCRSA_GENERATE_KEY_CONSISTENCY" returned for RSA Error code "CCDH_GENERATE_KEY_CONSISTENCY" returned for Diffie-Hellman

Name	Description	Conditions	Recovery Method	Indicator
	not match the known value or 3) The signature failed to generate/verify successfully in the Conditional PCT. No cryptographic services are provided, and data output is prohibited			

Table 26: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Startup Procedures: The module is built into macOS Ventura v13 defined in Section 2 and delivered with device. There is no standalone delivery of the module as a software library.

Installation Process and Authentication Mechanisms: The vendor's internal development process guarantees that the correct version of module goes with its intended macOS version. For additional assurance, the module is digitally signed by vendor, and it is verified during the integration into macOS.

This digital signature-based integrity protection during the delivery/integration process is not to be confused with the HMAC-SHA2-256 based integrity check performed by the module itself as part of its pre-operational self- tests.

11.2 Administrator Guidance

The Approved mode of operation is configured in the system 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. If the device starts up successfully, then the module has passed all self-tests and is operating in the Approved mode.

Apple Platform Certifications guide (platform certifications) and Apple Platform Security guide (SEC) are provided by Apple which offers IT System Administrators with the necessary technical information to ensure FIPS 140-3 Compliance of the deployed systems. This guide walks the reader through the system's assertion of cryptographic module integrity and the steps necessary if module integrity requires remediation.

11.3 Non-Administrator Guidance

None.

11.4 Design and Rules

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

- AES-GCM see Section 2.7.
- AES-XTS see Section 2.7.
- PBKDF see Section 2.7.

IG C.F Compliance: All of the RSA modulus sizes used by the cryptographic module have been CAVP tested, and the certificates are listed in the Approved Algorithms Table of this security policy. There are no untested RSA modulus sizes used by the cryptographic module.

11.5 End of Life

The module secure sanitization is accomplished by first powering the module down, which will zeroize all SSPs within volatile memory. Following the power-down, an uninstall by way of system wipe or system update will zeroize the corecrypto binary file.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.