Apple Inc.

Apple corecrypto Module v14.0 [Intel, Kernel, Software, SL1]

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
March 13th, 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 v14.0 [Intel, Kernel, 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 Sonoma v14) kernels 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 kernel space and does not contain any terminating assertions or exceptions. It is implemented as a Host OS dynamically loadable library. The library is loaded into the Host OS kernel and its cryptographic functions are made available to Host OS kernel services only.

Any internal error detected by the module is returned to the caller with an appropriate return code. The calling Host OS kernel 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: MultiChipStand

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 kernel space of the computing platforms and operating systems listed in the Tested Operational Environments Table.

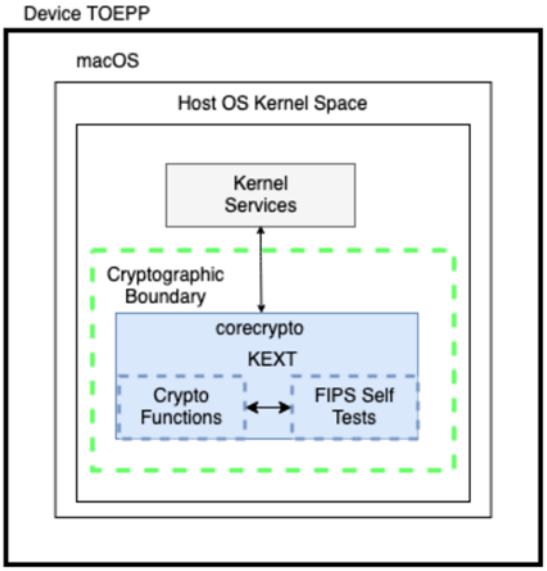

Figure 1: Block Diagram

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
xnu-10002.60.75.0.3	v14.0	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 Sonoma v14	MacBook Pro	Intel i5 (Coffee Lake 8257U)	Yes	N/A	v14.0
macOS Sonoma v14	iMac	Intel i5 (Comet Lake 10500)	Yes	N/A	v14.0
macOS Sonoma v14	MacBook Air	Intel i5 (Amber Lake 8210Y)	Yes	N/A	v14.0
macOS Sonoma v14	MacBook Pro	Intel i7 (Coffee Lake 8569U)	Yes	N/A	v14.0
macOS Sonoma v14	iMac	Intel i7 (Comet Lake 10700K)	Yes	N/A	v14.0
macOS Sonoma v14	iMac	Intel i7 (Comet Lake 10700K)	No	N/A	v14.0
macOS Sonoma v14	MacBook Pro	Intel i7 (Ice Lake 1060NG7)	Yes	N/A	v14.0
macOS Sonoma v14	MacBook Pro	Intel i9 (Coffee Lake 9880H)	Yes	N/A	v14.0
macOS Sonoma v14	iMac	Intel i9 (Comet Lake 10910)	Yes	N/A	v14.0
macOS Sonoma v14	iMac	Intel i9 (Comet Lake 10910)	No	N/A	v14.0
macOS Sonoma v14	Mac Pro	Xeon W (Cascade Lake W-3223)	Yes	N/A	v14.0

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

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

N/A for this module.

2.3 Excluded Components

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 '0' 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 any non-zero value 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 4: 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	A6208	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6209	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6204	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6205	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6204	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6205	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6204	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6205	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6208	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6209	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6204	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6205	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KW	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A6210	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A6211	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A6208	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6209	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A6204	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6205	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6210	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6211	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A6201	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A6202	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A6212	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A6201	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A6202	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A6212	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A6201	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)	A6202	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)	A6212	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)	A6201	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)	A6202	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)	A6212	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	A6201	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A6202	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A6212	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6207	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6207	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6207	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6207	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6207	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6201	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6202	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6212	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KDF SP800-108	A6202	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
RSA SigGen (FIPS186-4)	A6201	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A6202	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A6212	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6201	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6202	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6212	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA-1	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6207	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6207	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6207	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6207	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6207	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6201	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6202	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6212	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
TDES-ECB	A6203	Direction - Decrypt, Encrypt	SP 800-67 Rev. 2

Table 5: 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 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

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

Name	Use and Function
ANSI X9.63 KDF	Hash based Key Derivation Function
Blowfish	Encryption/Decryption
CAST5	Encryption/Decryption Key Sizes: 40 to 128 bits in 8-bit increments
DES	Encryption/Decryption Key Size: 56-bits
ECDSA	PKG: Curve P-192; PKV: Curve P-192; compact point representation of points; Signature Generation: Curve P-192; Signature Verification: Curve P-192
Ed25519	Key Generation, Signature Generation, Signature Verification
HKDF [SP800-56Crev2]	Key Derivation Function
Integrated Encryption Scheme on elliptic curves	Encryption/Decryption
MD2	Message Digest size: 128-bit
MD4	Message Digest size: 128-bit
MD5	Message Digest
OMAC (One-Key CBC MAC)	MAC Generation/Verification
RC2	Encryption/Decryption
RC4	Encryption/Decryption
RIPEMD	Message Digest
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
Triple-DES [SP 800-67]	Encryption
RFC6637	Key Derivation Function

Table 7: 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-ECB: (A6204, A6205, A6208, A6209, A6210, A6211) AES-CBC: (A6208, A6209, A6210, A6211) AES-CFB8: (A6210, A6211)

Name	Type	Description	Properties	Algorithms
				AES-CFB128: (A6210, A6211) AES-CTR: (A6204, A6205, A6210, A6211) AES-OFB: (A6210, A6211) AES-XTS Testing Revision 2.0: (A6208, A6209)
AES Authenticated Cipher	BC-Auth	AES Authenticated Encryption and Decryption		AES-CCM: (A6204, A6205) AES-GCM: (A6204, A6205) AES-KW: (A6210, A6211)
MAC (HMAC)	MAC	HMAC Generation and Verification		HMAC-SHA-1: (A6201, A6202, A6207, A6212) HMAC-SHA2-224: (A6201, A6202, A6207, A6212) HMAC-SHA2-256: (A6201, A6202, A6207, A6212) HMAC-SHA2-384: (A6201, A6202, A6207, A6212) HMAC-SHA2-512: (A6201, A6202, A6207, A6212) HMAC-SHA2-512/256: (A6201, A6202, A6212)
Message Digest	SHA	SHA Digest		SHA-1: (A6201, A6202, A6207, A6212) SHA2-224: (A6201, A6202, A6207, A6212) SHA2-256: (A6201, A6202, A6207, A6212)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A6201, A6202, A6207, A6212) SHA2-512: (A6201, A6202, A6207, A6212) SHA2-512/256: (A6201, A6202, A6212)
Key Derivation	KBKDF	Key Derivation		KDF SP800-108: (A6202)
Random Bit Generation	DRBG	Random Bit Generation		Counter DRBG: (A6204, A6205, A6210, A6211) HMAC DRBG: (A6201, A6202, A6212)
ECC Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer CKG	ECDSA Asymmetric Key Pair Generation and Verification		ECDSA KeyGen (FIPS186-4): (A6201, A6202, A6212) ECDSA KeyVer (FIPS186-4): (A6201, A6202, A6212) CKG: () Key Type: Asymmetric
ECDSA Digital Signature	DigSig-SigGen DigSig-SigVer	ECDSA Digital Signature Generation and Verification		ECDSA SigGen (FIPS186-4): (A6201, A6202, A6212) ECDSA SigVer (FIPS186-4): (A6201, A6202, A6212)
RSA Digital Signature	DigSig-SigGen DigSig-SigVer	RSA Digital Signature Generation and Verification		RSA SigGen (FIPS186-4): (A6201, A6202, A6212) RSA SigVer (FIPS186-4): (A6201, A6202, A6212)
TDES Decryption	BC-UnAuth	TDES Symmetric Decryption		TDES-ECB: (A6203)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

GCM IV

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

The GCM IV generation follows RFC 4106 and shall only be used for the IPsec protocol version 3. When the IV in RFC 4106 exhausts the maximum number of possible values for a given security association, either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association. The module uses RFC 7296 compliant IKEv2 to establish the shared secret *SKEYSEED* from which the AES-GCM encryption keys are derived.

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. This condition is not enforced by the module.

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.

SHA-1 Usage:

SHA-1 is only Approved for legacy use with Digital Signature Verification. For non-digital signature applications, SHA-1 is disallowed for applying protection after 2030 and allowed only for legacy use for processing already protected information after 2030.

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.

2.8 RBG and Entropy

The tables below detail the modules ESV information.

Cert Number	Vendor Name
E14	apple
E181	apple

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Apple corecrypto physical entropy source	Physical	Apple T2 Security Chip (for Intel-based computers)	256 bits	256 bits	CTR_DRBG AES-256 [ACVP Cert. #DRBG 2029]
Apple corecrypto non-physical entropy source	Non-Physical	macOS Sonoma 14 on Intel Coffee Lake 8th Gen Intel(R) Core(TM) i5-8257U; macOS Sonoma 14 on Intel Comet Lake 10th Gen Intel(R) Core(TM) i5-10500; macOS	512 bits	512 bits	SHA2-512 [ACVP Cert #A6207]

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
		Sonoma 14 on Intel Amber Lake 8th Gen Intel(R) Core(TM) i5-8210Y; macOS Sonoma 14 on Intel Coffee Lake 8th Gen Intel(R) Core(TM) i7-8569U; macOS Sonoma 14 on Intel Comet Lake 10th Gen Intel(R) Core(TM) i7-10700K; macOS Sonoma 14 on Intel Ice Lake 10th Gen Intel(R) Core(TM) i7-1060NG7; macOS Sonoma 14 on Intel Coffee Lake 9th Gen Intel(R) Core(TM) i9-9880H; macOS Sonoma 14 on Intel Comet Lake 10th Gen Intel(R) Core(TM) i9-10910; macOS Sonoma 14 on Intel Cascade Lake Intel(R) Xeon(R) W-3223			

Table 10: 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 "*read_random*". The *read_random* is the Kernel 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 EC key pairs as well as the [SP 800-90Ar1] DRBG have been ACVT tested with algorithm certificates.

The module also implements KBKDF Key Derivation according to [SP 800-108r1] to derive symmetric keys. The module supports Counter mode with 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 does not implement any approved key establishment methods.

2.11 Industry Protocols

No parts of the IPsec protocol, 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 C language Kernel Interfaces (KPIs) and callable service invocations, generally through caller-supplied buffers.
N/A	Data Output	Data outputs are provided in the variables passed in the C language Kernel Interfaces (KPIs) 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 KPI lists possible return codes. A complete list of all return codes returned by the C language KPIs within the module is provided in the header files and the KPI documentation. Messages are also documented in the KPI documentation.

Table 11: 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 12: 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
AES Encryption/Decryption	Execute AES-mode encrypt or decrypt operation	0	Plaintext data and key / Ciphertext data and key	Ciphertext data / Plaintext data	AES Cipher AES Authenticated Cipher	Crypto Officer - AES Key: W,E
AES Key Wrapping/Key unwrapping	Execute AES-key wrapping or unwrapping operation	0	AES key wrapping key, key to be wrapped / Wrapped key, AES key wrapping key	Wrapped key / Unwrapped key	AES Authenticated Cipher	Crypto Officer - AES Key-Wrapping Key: W,E
Secure Hash Generation	Generate a digest for the requested algorithm	0	Message	Digest	Message Digest	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Authentication Generation	Generate a MAC digest using the requested SHA algorithm	0	Message, MAC key, MAC algorithm	MAC	MAC (HMAC)	Crypto Officer - HMAC Key: W,E
Message Authentication Verification	Verify a MAC digest	0	MAC, message, MAC key, MAC algorithm	Pass/Fail	MAC (HMAC)	Crypto Officer - HMAC Key: W,E
Key Derivation (KDF)	Derive key from key derivation key	0	KDF key derivation key	KDF derived key	Key Derivation	Crypto Officer - KDF Key Derivation Key: W,E - KDF Derived Key: G,R
Random Number Generation	Generate random number	0	Requested number of bits	Random bit-string	Random Bit Generation	Crypto Officer - Entropy Input String: W,E - DRBG Seed, Internal State V, and Key (IG D.L): G,E
ECDSA Key Pair Generation	Generate a keypair for a requested elliptic curve	0	Curve size	ECDSA Key pair	ECC Key Generation	Crypto Officer - DRBG Seed, Internal State V, and Key (IG D.L): E -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Private Key: G,R - ECDSA Public Key: G,R
ECDSA Signature Generation and Verification	Sign a message with a specified ECDSA private key / Verify the signature of a message with a specified ECDSA public key	0	SigGen: private key, message, hash function / SigVer: public key, digital signature, message, hash function	SigGen: computed signature / SigVer: Pass/Fail result of digital signature verification	ECDSA Digital Signature	Crypto Officer - ECDSA Private Key: W,E - ECDSA Public Key: W,E
RSA Signature Generation and Verification	Sign a message with a specified RSA private key / Verify the signature of a message with a specified RSA public key	0	SigGen: private key, message, hash function / SigVer: public key, digital signature, message, hash function	SigGen: computed signature / SigVer: Pass/Fail result of digital signature verification	RSA Digital Signature	Crypto Officer - RSA Private Key: W,E - RSA Public Key: W,E
TDES Decryption	Execute TDES-mode decrypt operation	0	Ciphertext data and key	Plaintext data	TDES Decryption	Crypto Officer - TDES Key: W,E
On-Demand Self-test	Execute on-demand self-tests	N/A	N/A	Pass or Fail	AES Cipher AES Authenticated Cipher	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	by rebooting the module				MAC (HMAC) Message Digest Key Derivation Random Bit Generation ECC Key Generation ECDSA Digital Signature RSA Digital Signature TDES Decryption	
Show Status	Return the module status	N/A	N/A	Module status	None	Crypto Officer
Show Module and Version Information	Return Module Base Name and Module Version Number	N/A	N/A	Module information	None	Crypto Officer
Zeroisation	Zeroise all SSPs	0	Length of context to zeroize and address of context to be zeroized	N/A	None	Crypto Officer - AES Key: Z - AES Key-Wrapping Key: Z - HMAC Key: Z - KDF Key Derivation Key: Z - KDF Derived Key: Z - Entropy Input String: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed, Internal State V, and Key (IG D.L): Z - ECDSA Private Key: Z - ECDSA Public Key: Z - RSA Private Key: Z - RSA Public Key: Z - TDES Key: Z

Table 13: Approved Services

4.4 Non-Approved Services

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

Name	Description	Algorithms	Role
ANSI X9.63 KDF	Hash based Key Derivation Function	ANSI X9.63 KDF	CO
Blowfish	Encryption and Decryption	Blowfish	CO
CAST5	Encryption and Decryption	CAST5	CO
DES	Encryption and Decryption	DES	CO
ECDSA	PKG: Curve P-192; PKV: Curve P-192; compact point representation of points; Signature Generation: Curve P-192; Signature Verification: Curve P-192	ECDSA	CO
Ed25519	Key Generation, Signature Generation, Signature Verification	Ed25519	CO
SP800-56Crev2 Key Derivation (HKDF)	Key Derivation Function	HKDF [SP800-56Crev2]	CO
Encryption Scheme on elliptic curves	Encryption and Decryption	Integrated Encryption Scheme on elliptic curves	CO
MD2	Message Digest size: 128-bit	MD2	CO
MD4	Message Digest size: 128-bit	MD4	CO
MD5	Message Digest size: 128-bit	MD5	CO

Name	Description	Algorithms	Role
OMAC (One-Key CBC MAC)	MAC Generation	OMAC (One-Key CBC MAC)	CO
RC2	Encryption and Decryption	RC2	CO
RC4	Encryption and Decryption	RC4	CO
RIPEMD	Message Digest size: 160-bits	RIPEMD	CO
RSA Digital Signature	PKCS#1 v1.5 and PSS; Signature Generation Key Size < 2048; Signature Verification Key Size < 1024	RSA Digital Signature	CO
RSA Key Wrapping	OAEP, PKCS#1 v1.5 and PSS schemes	RSA Key Wrapping	CO
Triple-DES [SP 800-67]	Encryption	Triple-DES [SP 800-67]	CO
RFC6637	Key Derivation Function	RFC6637	CO

Table 14: 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 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 Host OS, 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 v14.0 [Intel, Kernel, 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 15: 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
KPI input parameters	Operator calling application (TOEPP)	RAM	Plaintext	Manual	Electronic	
KPI output parameters	RAM	Operator calling application (TOEPP)	Plaintext	Manual	Electronic	

Table 16: 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
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded.	By calling the cipher related zeroization API.

Zeroization Method	Description	Rationale	Operator Initiation
Module Reset	De-allocates the volatile memory used to store SSPs.	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module.
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 17: 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
AES Key-Wrapping Key	AES-KW key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Authenticated Cipher
HMAC Key	HMAC key	128 to 256 bits - 128 to 256 bits	MAC Key - CSP			MAC (HMAC)
KDF Key Derivation Key	KDF key derivation key	128 to 256 bits - 128 to 256 bits	Derivation Key - CSP			Key Derivation
KDF Derived Key	KDF derived key	128 to 256 bits - 128 to 256 bits	Derived Key - CSP	Key Derivation		
Entropy Input String	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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
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
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
RSA Private Key	RSA private key	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - CSP			RSA Digital Signature
RSA Public Key	RSA public key	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - PSP			RSA Digital Signature
TDES Key	TDES key	168 bits - 112 bits	Symmetric Key - CSP			TDES Decryption

Table 18: SSP Table 1

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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KDF Key Derivation Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	KDF Derived Key:Derives
KDF Derived Key	KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	KDF Key Derivation Key:Derived From
Entropy Input String	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Module Reset	DRBG Seed, Internal State V, and Key:Generates
DRBG Seed, Internal State V, and Key (IG D.L)		RAM:Plaintext	From service invocation to service completion	Module Reset	Entropy Input String:Generated From
ECDSA Private Key	KPI input parameters KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset Intermediate value zeroization	ECDSA Public Key:Paired With
ECDSA Public Key	KPI input parameters KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset Intermediate value zeroization	ECDSA Private Key:Paired With
RSA Private Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RSA Public Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA Private Key:Paired With
TDES Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	

Table 19: SSP Table 2

9.5 Transitions

Please see the latest revision of SP 800-131A and CMVP Programmatic Transitions page for transitions that may affect this module.

Per NIST SP 800-131A rev3, usage of the SHA-1 service as part of Digital Signature Generation is disallowed in the approved mode of operation. SHA-1 is only Approved for legacy use with Digital Signature Verification. For non-digital signature applications, SHA-1 is disallowed for applying protection after 2030 and allowed only for legacy use for processing already protected information after 2030. SHA-1 is disallowed for HMAC Generation (≥ 112 bits) after 2030 and allowed only for legacy use for HMAC Verification (≥ 112 bits) after 2030.

Per FIPS 140-3, IG C.K FIPS 186-4 CAVP tests performed are mathematically identical to FIPS 186-5 CAVP tests, therefore the module can claim FIPS 186-5 compliance for these tests.

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 (A6207)	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 20: 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
AES-GCM (A6204)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A6205)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A6204)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A6205)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
Counter DRBG (A6204)	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 (A6205)	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 (A6210)	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 (A6211)	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 (A6201)	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 (A6202)	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 (A6212)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on after the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
HMAC-SHA-1 (A6201)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6202)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6207)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6212)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6201)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6202)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6207)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on before the integrity test
HMAC-SHA2-	SHA2-256	KAT	CAST	Module becomes	Message Authentication	Test runs at power-on after

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
256 (A6212)				operational		the integrity test
HMAC-SHA2-512 (A6201)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6202)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6207)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6212)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6201)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6202)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6212)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
RSA SigGen	PKCS#1v1.5 with 2048 bit	KAT	CAST	Module becomes	Digital Signature Generation	Test runs at power-

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-4) (A6201)	key and SHA2-256			operational		on after the integrity test
RSA SigGen (FIPS186-4) (A6202)	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 SigGen (FIPS186-4) (A6212)	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) (A6201)	PKCS#1v1.5 with 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) (A6202)	PKCS#1v1.5 with 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) (A6212)	PKCS#1v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA KeyGen (FIPS186-4) (A6201)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A6202)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186	PCT	PCT	PCT	Successful key pair	Key Generation	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
-4) (A6212)				generation		
ECDSA SigGen (FIPS186-4) (A6201)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A6202)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A6212)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A6201)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A6202)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A6212)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
KDF SP800-108 (A6202)	Counter mode KDF with 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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A6208)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A6209)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A6210)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A6211)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A6204)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A6205)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A6208)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A6209)	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-ECB (A6210)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A6211)	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 (A6208)	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 (A6209)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
TDES-ECB (A6203)	Keying Option 1, decrypt	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test

Table 21: 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 rebooting the module which runs the On-Demand Self-test service.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6207)	Message Authentication over the complete module file image	SW/FW Integrity	Whenever module is powered on	Upon every power on

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A6204)	KAT	CAST	On Demand	Power cycle
AES-GCM (A6205)	KAT	CAST	On Demand	Power cycle
AES-CCM (A6204)	KAT	CAST	On Demand	Power cycle
AES-CCM (A6205)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6204)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6205)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6210)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6211)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6201)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6202)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6212)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6201)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6202)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6207)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6212)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6201)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6202)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6207)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6212)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6201)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6202)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6207)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6212)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6201)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6202)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6212)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6201)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6202)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6212)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6201)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6202)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6212)	KAT	CAST	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6201)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6202)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6212)	PCT	PCT	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A6201)	KAT	CAST	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-4) (A6202)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A6212)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6201)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6202)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6212)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A6202)	KAT	CAST	On Demand	Power cycle
AES-CBC (A6208)	KAT	CAST	On Demand	Power cycle
AES-CBC (A6209)	KAT	CAST	On Demand	Power cycle
AES-CBC (A6210)	KAT	CAST	On Demand	Power cycle
AES-CBC (A6211)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6204)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6205)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6208)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6209)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6210)	KAT	CAST	On Demand	Power cycle
AES-ECB (A6211)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6208)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6209)	KAT	CAST	On Demand	Power cycle
TDES-ECB (A6203)	KAT	CAST	On Demand	Power cycle

Table 23: 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 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	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 Error code

Table 24: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Startup Procedures: The module is built into Host OS defined in Section 2 and delivered/installed with the respective Host OS. 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 Host OS version. For additional assurance, the module is digitally signed by vendor, and it is verified during the integration into Host OS.

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.
- SHA-1 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 xnu binary file.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.