Apple Inc.

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

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
May 21st, 2026

Prepared by:

Lightship Security

Applus

www.lightshipsec.com

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Table of Contents

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

List of Tables

List of Figures

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Apple corecrypto Module v13.0 [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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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) 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: 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 kernel space of the computing platforms and operating systems listed in the Tested Operational Environments Table and Vendor-Affirmed Operational Environments Table.

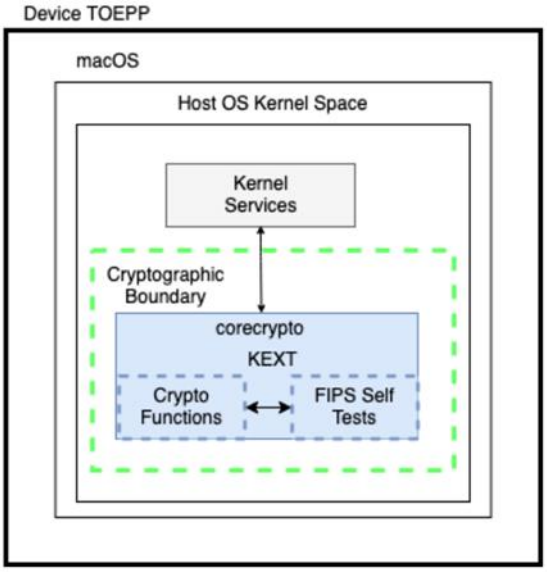

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

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

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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-8792.81.3	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

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

This document may be reproduced and distributed only in its original entirety without revision.

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	A3618	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3619	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3620	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3626	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	A3627	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96,	SP 800-38C

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
		104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	
AES-CFB128	A3620	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3620	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A3620	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	A3621	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	A3626	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	A3627	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	A3618	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3619	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3620	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A3626	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A3627	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3626	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	A3627	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	A3620	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-KW	A3621	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128-4096 Increment 128	SP 800-38F
AES-OFB	A3620	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A3621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A3618	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	A3619	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

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A3620	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	A3621	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	A3626	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	A3627	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	SP 800-90A Rev. 1

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
		Personalization String Length - Personalization String Length: 0, 128, Personalization String Length: 0, 256 Returned Bits - 128	
ECDSA KeyGen (FIPS186-4)	A3622	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3623	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3624	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3622	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3623	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3624	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3622	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)	A3623	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)	A3624	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)	A3622	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)	A3623	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)	A3624	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	A3622	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

This document may be reproduced and distributed only in its original entirety without revision.

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	A3623	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	A3624	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	A3622	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3623	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3624	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A3628	MAC - MAC: 160 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-224	A3622	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3623	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3624	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3628	MAC - MAC: 224 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3622	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3623	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3624	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3628	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3622	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3623	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3624	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3628	MAC - MAC: 384 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3622	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3623	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3624	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3628	MAC - MAC: 512 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512/256	A3622	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3623	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A3624	MAC - MAC: 256 Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KDF SP800-108	A3624	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
RSA KeyGen (FIPS186-4)	A3622	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)	A3623	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)	A3624	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)	A3622	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigGen (FIPS186-4)	A3623	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigGen (FIPS186-4)	A3624	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
		Hash Pair - Hash Algorithm - SHA2-224	
RSA SigVer (FIPS186-4)	A3622	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)	A3623	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)	A3624	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
SHA-1	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A3628	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A3628	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A3628	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A3628	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A3628	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3622	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3623	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A3624	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
TDES-ECB	A3625	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:

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
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
X25519	Key Agreement; Key Generation
Ed25519	Key Generation; Signature Generation; Signature Verification

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Use and Function
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; Digest size 128-bit
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 2^16 encryptions with the same Triple-DES key, as required by FIPS 140-3 IG C.G.

Table 8: 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: (A3618, A3619, A3620, A3621) AES-CFB8: (A3620, A3621) AES-CTR: (A3620, A3621, A3626, A3627) AES-ECB: (A3618, A3619, A3620, A3621, A3626, A3627) AES-OFB: (A3620, A3621) AES-XTS Testing Revision 2.0: (A3618, A3619)

This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
				AES-CFB128: (A3620, A3621)
TDES Decryption	BC-UnAuthDecrypt	TDES Symmetric Decryption		TDES-ECB: (A3625)
AES Authenticated Cipher	BC-Auth	AES Authenticated Encryption and Decryption		AES-CCM: (A3626, A3627) AES-GCM: (A3626, A3627) AES-KW: (A3620, A3621)
Random Bit Generation	DRBG	Random Bit Generation		Counter DRBG: (A3620, A3621, A3626, A3627) HMAC DRBG: (A3622, A3623, A3624)
ECC Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer CKG	ECDSA Asymmetric Key Pair Generation and Verification		ECDSA KeyGen (FIPS186-4): (A3622, A3623, A3624) ECDSA KeyVer (FIPS186-4): (A3622, A3623, A3624) CKG: () Key Type: Asymmetric
RSA Key Generation	AsymKeyPair-KeyGen CKG	RSA Asymmetric Key Pair Generation		RSA KeyGen (FIPS186-4): (A3622, A3623, A3624) CKG: () Key Type: Asymmetric
ECDSA Digital Signature	DigSig-SigGen DigSig-SigVer	ECDSA Digital Signature Generation and Verification		ECDSA SigGen (FIPS186-4): (A3622, A3623, A3624) ECDSA SigVer (FIPS186-4): (A3622, A3623, A3624)
RSA Digital Signature	DigSig-SigGen DigSig-SigVer	RSA Digital Signature Generation and Verification		RSA SigGen (FIPS186-4): (A3622, A3623, A3624) RSA SigVer (FIPS186-4):

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Type	Description	Properties	Algorithms
				(A3622, A3623, A3624)
Message Digest	SHA	SHA Digest		SHA-1: (A3622, A3623, A3624, A3628) SHA2-224: (A3622, A3623, A3624, A3628) SHA2-256: (A3622, A3623, A3624, A3628) SHA2-384: (A3622, A3623, A3624, A3628) SHA2-512: (A3622, A3623, A3624, A3628) SHA2-512/256: (A3622, A3623, A3624)
MAC (HMAC)	MAC	HMAC Generation and Verification		HMAC-SHA-1: (A3622, A3623, A3624, A3628) HMAC-SHA2-224: (A3622, A3623, A3624, A3628) HMAC-SHA2-256: (A3622, A3623, A3624, A3628) HMAC-SHA2-384: (A3622, A3623, A3624, A3628) HMAC-SHA2-512: (A3622, A3623, A3624, A3628) HMAC-SHA2-512/256: (A3622, A3623, A3624)
Key Derivation	KBKDF	Key Derivation		KDF SP800-108: (A3624)

Table 9: Security Function Implementations

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

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
E110	apple

Table 10: 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 11: 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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 RSA, 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 both Counter and Feedback modes 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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 KPI and callable service invocations, generally through caller-supplied buffers.
N/A	Data Output	Data inputs are provided in the variables passed in the KPI 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, namely the kernel module plist whose information is supplied to the module by the kernel module loader.
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 12: Ports and Interfaces

The module does not implement a Control Output Logical Interface.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 13: 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	AES Key; Plaintext data	Ciphertext data	AES Cipher AES Authenticated Cipher	Crypto Officer - AES key: W,E - AES GCM key: W,E - AES XTS key: W,E
Symmetric decryption	Decrypt ciphertext data	1	AES/TDES Key; Ciphertext data	Plaintext data	AES Cipher TDES Decryption AES Authenticated Cipher	Crypto Officer - AES key: W,E - AES GCM key: W,E - AES XTS key: W,E - TDES Key: W,E

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Key wrapping	Perform key wrapping	1	Key-encryption-key; Key to be wrapped	Wrapped key	AES Authenticated Cipher	Crypto Officer - AES Key-Encrypting Key: W,E
Key unwrapping	Perform key unwrapping	1	Key-encryption-key; Wrapped key	Unwrapped key	AES Authenticated Cipher	Crypto Officer - AES Key-Encrypting Key: W,E
Hashing	Compute a message digest	1	Message	Message digest	Message Digest	Crypto Officer
MAC Generation	Compute a message authentication code	1	Message, MAC key, MAC algorithm	Message Authentication Code	MAC (HMAC)	Crypto Officer - HMAC key: W,E
MAC Verification	Verify a message authentication code	1	MAC, message, HMAC key, MAC algorithm	Pass/fail result	MAC (HMAC)	Crypto Officer - HMAC key: W,E
Derive key via KBKDF	Derive keys	1	KBKDF Key Derivation Key	Derived key	Key Derivation	Crypto Officer - KBKDF Key derivation key: W,E - KBKDF Derived key: G,R
ECDSA key pair generation	Generate a public/private key pair	1	Random numbers, domain parameters	Public/private key pair	ECC Key Generation	Crypto Officer - ECDSA public key: G,R - ECDSA private key: G,R
ECDSA signature generation	Generate a digital signature	1	Private key, message,	Digital signature	ECDSA Digital Signature	Crypto Officer - ECDSA

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			hash function			private key: E
ECDSA signature verification	Verify a digital signature	1	Public key	True or False	ECDSA Digital Signature	Crypto Officer - ECDSA public key: W,E
RSA key pair generation	Generate a public/private key pair	1	Random numbers, domain parameters	Public/private key pair	RSA 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	Digital signature	RSA Digital Signature	Crypto Officer - RSA private key: E
RSA signature verification	Verify a digital signature	1	Public key	True or False	RSA Digital Signature	Crypto Officer - RSA public key: W,E
Random number generation	Generate a random number	1	Entropy, seed, V and key values	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
Zeroisation	Zeroise all SSPs	1	Length of context to zeroize and address of context to be zeroized	Released memory space	None	Crypto Officer - AES key: Z - AES Key-Encrypting Key: Z - AES GCM

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key: Z - AES XTS key: Z - HMAC key: Z - ECDSA public key: Z - ECDSA private key: Z - RSA public key: Z - RSA private key: Z - Entropy Input String: Z - DRBG Seed, Internal State V, and Key (IG D.L): Z - KBKDF Key derivation key: Z - KBKDF Derived key: Z - TDES Key: Z
On-Demand Self-test	Perform pre-operational and algorithm self-test	1	Instantiation	Status	AES Cipher TDES Decryption AES Authenticated Cipher Random Bit Generation ECC Key Generation RSA Key Generation	Crypto Officer

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ECDSA Digital Signature RSA Digital Signature Message Digest MAC (HMAC) Key Derivation	
Show Status	Return module status	N/A	KPI invocation	Operational/error status	None	Crypto Officer
Show Module and Version Information	Return module name and versioning information	N/A	KPI invocation	Module base name; Module version	None	Crypto Officer

Table 14: Approved Services

4.4 Non-Approved Services

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

Name	Description	Algorithms	Role
Key Encapsulation	Perform key wrapping	RSA Key Wrapping	CO
Key Decapsulation	Perform key unwrapping	RSA Key Wrapping	CO
EdDSA/X25519 key pair generation	Generate a public/private key pair; Curve: Ed25519 and Curve25519	X25519 Ed25519	CO
EdDSA signature generation	Generate a digital signature; Curve: Ed25519	Ed25519	CO
EdDSA signature verification	Verify a digital signature; Curve: Ed25519	Ed25519	CO
X25519 key agreement	Perform key agreement	X25519	CO
ECDSA key pair generation	Generate a public/private key pair; Curve: P-192	ECDSA	CO
ECDSA signature generation	Generate a digital signature; Curve: P-192	ECDSA	CO
ECDSA Signature verification	Verify a digital signature; Curve: P-192	ECDSA	CO
RSA key pair generation	Generate a public/private key pair; Key size < 2048	RSA Key Generation	CO
RSA signature generation	Generate a digital signature; Key size < 2048	RSA Digital Signature	CO

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Algorithms	Role
RSA Signature verification	Verify a digital signature; Key size < 1024	RSA Digital Signature	CO
ANSI X9.63 KDF Key Derivation	Hash-based key derivation; Per: ANSI X9.63	ANSI X9.63 KDF	CO
SP 800-56C HKDF Key Derivation	Hash-based key derivation; Per: SP 800-56C HKDF	HKDF [SP 800-56C]	CO
RFC6637 Key Derivation	Hash-based key derivation; Per: RFC6637	RFC6637	CO
Generate MAC	Compute a message authentication code	OMAC (One-Key CBC MAC)	CO
Hashing	Compute a message digest	MD2 MD4 MD5 RIPEMD	CO
Symmetric encryption	Perform symmetric data encryption	DES CAST5 RC4 RC2 Integrated Encryption Scheme on elliptic curves (ECIES) Blowfish Triple-DES [SP 800-67r2]	CO
Symmetric decryption	Perform symmetric data decryption	DES CAST5 RC4 RC2 Integrated Encryption Scheme on elliptic curves (ECIES) Blowfish Triple-DES [SP 800-67r2]	CO

Table 15: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support external software loaded.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

7 Physical Security

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

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 16: 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 17: 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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 18: 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-Encrypting Key	AES-KW key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Authenticated Cipher
AES GCM key	AES-GCM key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Authenticated Cipher
AES XTS key	AES-XTS key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Cipher
HMAC key	HMAC key	>=112 bits - >=112 bits	MAC Key - CSP			MAC (HMAC)
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 intermediat	P-224, P-256, P-384, P-521 -	Asymmetric Key - CSP	ECC Key Generation		ECDSA Digital Signature

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	e keygen values)	112 to 256 bits				
RSA public key	RSA public key	2048 to 4096 bits - 112 to 256 bits	Asymmetric Key - PSP	RSA Key Generation		RSA Digital Signature
RSA private key	RSA private key	2048 to 4096 bits - 112 to 256 bits	Asymmetric Key - CSP	RSA Key Generation		RSA Digital Signature
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
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		
TDES Key	TDES key	168 bits - 112 bits	Symmetric Key - CSP			TDES Decryption

Table 19: 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-Encrypting Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated	

This document may be reproduced and distributed only in its original entirety without revision.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Module Reset	
AES GCM key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
AES XTS 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	
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
ECDSA private key	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
RSA public key	KPI input parameters KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	RSA private key:Paired With
RSA private key	KPI output parameters	RAM:Plaintext	From service invocation	Wipe and Free memory block allocated	RSA public key:Paired With

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			to service completion	Module Reset	
Entropy Input String	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Module Reset	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	Module Reset	Entropy Input String:Generated From
KBKDF Key derivation key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	KBKDF Derived key:Derives
KBKDF Derived key	KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	KBKDF Key derivation key:Derived From
TDES Key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	

Table 20: SSP Table 2

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 (A3628)	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 21: 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 (A3622)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A3623)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A3624)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A3628)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on before the integrity test
AES-CBC (A3618)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3619)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3620)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CBC (A3621)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3626)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-CCM (A3627)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3618)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
AES-ECB (A3619)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3620)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3621)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3626)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-ECB (A3627)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3626)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Authenticated Encryption/Decryption	Test runs at power-on after the integrity test
AES-GCM (A3627)	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	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes	Symmetric Encryption/Decryption	Test runs at power-on after

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
2.0 (A3618)				operational		the integrity test
AES-XTS Testing Revision 2.0 (A3619)	128-bit key, encrypt/decrypt	KAT	CAST	Module becomes operational	Symmetric Encryption/Decryption	Test runs at power-on after the integrity test
AES-KW (A3620)	128-bit key, wrap/unwrap	KAT	CAST	Module becomes operational	Key Wrapping/Unwrapping	Test runs at power-on after the integrity test
AES-KW (A3621)	128-bit key, wrap/unwrap	KAT	CAST	Module becomes operational	Key Wrapping/Unwrapping	Test runs at power-on after the integrity test
Counter DRBG (A3620)	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 (A3621)	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 (A3626)	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 (A3627)	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

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (A3622)	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 (A3623)	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 (A3624)	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 (A3622)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3623)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3624)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A3628)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3622)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						integrity test
HMAC-SHA2-512 (A3623)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3624)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A3628)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3622)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3623)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigGen (FIPS186-4) (A3624)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
RSA SigVer (FIPS186-4) (A3622)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
RSA SigVer (FIPS186	2048-bit modulus with SHA-256	KAT	CAST	Module becomes	Digital Signature Verification	Test runs at power-on after

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
-4) (A3623)				operational		the integrity test
RSA SigVer (FIPS186-4) (A3624)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A3622)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A3623)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-4) (A3624)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3622)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3623)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-4) (A3624)	P-256 curve with SHA-256	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test

This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SP800-108 (A3624)	Counter and Feedback modes	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
TDES-ECB (A3625)	168-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
ECDSA KeyGen (FIPS186-4) (A3622)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3623)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A3624)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A3622)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A3623)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A3624)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

Table 22: 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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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 (A3628)	Message Authentication over the complete module file image	SW/FW Integrity	Whenever module is powered on	Upon every power on

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3622)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3623)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3624)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A3628)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3618)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3619)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3620)	KAT	CAST	On Demand	Power cycle
AES-CBC (A3621)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3626)	KAT	CAST	On Demand	Power cycle
AES-CCM (A3627)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3618)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3619)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3620)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3621)	KAT	CAST	On Demand	Power cycle

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3626)	KAT	CAST	On Demand	Power cycle
AES-ECB (A3627)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3626)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3627)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3618)	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A3619)	KAT	CAST	On Demand	Power cycle
AES-KW (A3620)	KAT	CAST	On Demand	Power cycle
AES-KW (A3621)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3620)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3621)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3626)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A3627)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3622)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3623)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A3624)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3622)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3623)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3624)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A3628)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3622)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3623)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3624)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A3628)	KAT	CAST	On Demand	Power cycle

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A3622)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3623)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A3624)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3622)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3623)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A3624)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3622)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3623)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A3624)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3622)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3623)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A3624)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3624)	KAT	CAST	On Demand	Power cycle
TDES-ECB (A3625)	KAT	CAST	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A3622)	PCT	PCT	On Demand	On generating keys for ECDSA
ECDSA KeyGen (FIPS186-4) (A3623)	PCT	PCT	On Demand	On generating keys for ECDSA

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-4) (A3624)	PCT	PCT	On Demand	On generating keys for ECDSA
RSA KeyGen (FIPS186-4) (A3622)	PCT	PCT	On Demand	On generating keys for RSA
RSA KeyGen (FIPS186-4) (A3623)	PCT	PCT	On Demand	On generating keys for RSA
RSA KeyGen (FIPS186-4) (A3624)	PCT	PCT	On Demand	On generating keys for RSA

Table 24: 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	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 and Error code "CCRSA_GENERATE_KEY_CONSISTENCY" returned for RSA Error code"

This document may be reproduced and distributed only in its original entirety without revision.

Name	Description	Conditions	Recovery Method	Indicator
	cryptographic services are provided, and data output is prohibited			

Table 25: Error States

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

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.

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.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.

Apple Inc. 2026
This document may be reproduced and distributed only in its original entirety without revision.