Apple Inc.

Apple corecrypto Module v18.3 [Intel, User, Software, SL1]

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
March 25th, 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

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 21
2.7 Algorithm Specific Information 25
2.8 RBG and Entropy 26
2.9 Key Generation 27
2.10 Key Establishment 28
2.11 Industry Protocols 28
3 Cryptographic Module Interfaces 29
3.1 Ports and Interfaces 29
4 Roles, Services, and Authentication 30
4.1 Authentication Methods 30
4.2 Roles 30
4.3 Approved Services 30
4.4 Non-Approved Services 36
4.5 External Software/Firmware Loaded 37
5 Software/Firmware Security 38
5.1 Integrity Techniques 38
5.2 Initiate on Demand 38
6 Operational Environment 39
6.1 Operational Environment Type and Requirements 39
6.2 Configuration Settings and Restrictions 39
7 Physical Security 40
8 Non-Invasive Security 41
9 Sensitive Security Parameters Management 42
9.1 Storage Areas 42
9.2 SSP Input-Output Methods 42

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

9.3 SSP Zeroization Methods 42
9.4 SSPs 43
9.5 Transitions 47
10 Self-Tests 49
10.1 Pre-Operational Self-Tests 49
10.2 Conditional Self-Tests 49
10.3 Periodic Self-Test Information 64
10.4 Error States 72
11 Life-Cycle Assurance 74
11.1 Installation, Initialization, and Startup Procedures 74
11.2 Administrator Guidance 74
11.3 Non-Administrator Guidance 74
11.4 Design and Rules 74
11.5 End of Life 74
12 Mitigation of Other Attacks 75

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

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 7
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 7
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 8
Table 5: Modes List and Description 8
Table 6: Approved Algorithms 19
Table 7: Vendor-Affirmed Algorithms 19
Table 8: Non-Approved, Allowed Algorithms with No Security Claimed 20
Table 9: Non-Approved, Not Allowed Algorithms 21
Table 10: Security Function Implementations 25
Table 11: Entropy Certificates 26
Table 12: Entropy Sources 27
Table 13: Ports and Interfaces 29
Table 14: Roles 30
Table 15: Approved Services 36
Table 16: Non-Approved Services 37
Table 17: Storage Areas 42
Table 18: SSP Input-Output Methods 42
Table 19: SSP Zeroization Methods 43
Table 20: SSP Table 1 45
Table 21: SSP Table 2 47
Table 22: Pre-Operational Self-Tests 49
Table 23: Conditional Self-Tests 64
Table 24: Pre-Operational Periodic Information 64
Table 25: Conditional Periodic Information 72
Table 26: Error States 73

List of Figures

Figure 1: Block Diagram 6

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 v18.3 [Intel, User, Software, SL1], hereafter referred to as, “the module”. It contains the security rules under which the module must operate and describes how the module meets the requirements as specified in FIPS PUB 140-3 for an overall Security Level 1 cryptographic module.

1.2 Security Levels

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

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

Table 1: Security Levels

The Module has an overall security level of 1.

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 Sequoia v15) Security Framework and Common Crypto. The module provides services intended to protect data in transit and at rest.

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

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

Module Type: Software

Module Embodiment: 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 user space of the computing platforms and operating systems listed in the Tested Operational Environments Table and Vendor-Affirmed Operational Environments Table.

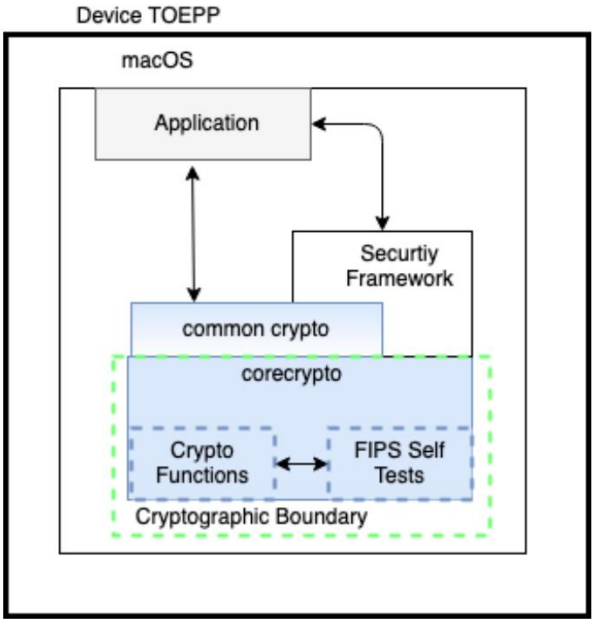

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

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

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
corecrypto-1736.80.2	v18.3	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 Sequoia v15	MacBook Pro 2019	Intel i9 (Coffee Lake 9880H)	Yes	N/A	v18.3
macOS Sequoia v15	MacBook Pro 2019	Intel i9 (Coffee Lake 9880H)	No	N/A	v18.3
macOS Sequoia v15	iMac 2020	Intel i9 (Comet Lake 10910)	Yes	N/A	v18.3
macOS Sequoia v15	iMac 2020	Intel i9 (Comet Lake 10910)	No	N/A	v18.3
macOS Sequoia v15	Mac Pro 2019	Xeon W (Cascade Lake W-3223)	Yes	N/A	v18.3
macOS Sequoia v15	Mac Pro 2019	Xeon W (Cascade Lake W-3223)	No	N/A	v18.3
macOS Sequoia v15	iMac Pro 2017	Xeon W (Skylake W-2140B)	Yes	N/A	v18.3
macOS Sequoia v15	iMac Pro 2017	Xeon W (Skylake W-2140B)	No	N/A	v18.3

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

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

Operating System	Hardware Platform
macOS Sequoia v15	Intel i5 (Coffee Lake 8257U) - MacBook Pro 2019
macOS Sequoia v15	Intel i5 (Comet Lake 10500) - iMac 2020
macOS Sequoia v15	Intel i5 (Amber Lake 8210Y) - MacBook Air 2018
macOS Sequoia v15	Intel i7 (Coffee Lake 8569U) - MacBook Pro 2019
macOS Sequoia v15	Intel i7 (Comet Lake 10700K) - iMac 2020
macOS Sequoia v15	Intel i7 (Ice Lake 1060NG7) - MacBook Air 2020

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

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

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

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

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

Mode Name	Description	Type	Status Indicator
Approved mode	Approved mode of operation is entered when the module utilizes the services that use the security functions listed in the Approved Algorithms Table and the Vendor Affirmed Algorithms Table.	Approved	Return a '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 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	A6489	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-CBC	A6490	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6496	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6491	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6492	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6497	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6498	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6499	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6497	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6498	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6499	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6489	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6490	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6492	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	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6498	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6499	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6491	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6492	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6497	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6498	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6499	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KW	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KW	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A6491	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A6492	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A6497	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A6489	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6490	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6491	Direction - Decrypt, Encrypt Key Length - 128, 256	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
AES-XTS Testing Revision 2.0	A6492	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6497	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A6491	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6492	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6497	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6498	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6499	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A6493	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A6494	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A6495	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A6497	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A6493	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6494	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6495	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6497	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-4)	A6493	Curve - P-224, P-256, P-384, P-521	FIPS 186-4

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

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyVer (FIPS186-4)	A6494	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A6495	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A6497	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-5)	A6493	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6494	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6495	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6497	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-4)	A6493	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)	A6494	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)	A6495	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)	A6497	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigGen (FIPS186-5)	A6493	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6494	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6495	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6497	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 Component - No	FIPS 186-5

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

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)	A6493	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)	A6494	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)	A6495	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)	A6497	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A6493	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6494	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6495	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6497	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5
HMAC DRBG	A6493	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A6494	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A6495	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A6497	Prediction Resistance - No Mode - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6500	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	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6493	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6494	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6495	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6497	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-SHA3-224	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-224	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6497	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6500	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6497	Domain Parameter Generation Methods - P-224, P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6497	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A6493	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDA HKDF SP800-56Cr2	A6494	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDA HKDF SP800-56Cr2	A6495	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-56C Rev. 2
KDA HKDF SP800-56Cr2	A6497	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	SP 800-56C Rev. 2

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

Algorithm	CAVP Cert	Properties	Reference
KDA HKDF SP800-56Cr2	A6500	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	SP 800-56C Rev. 2
KDF SP800-108	A6493	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A6494	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A6495	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A6497	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
PBKDF	A6493	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A6494	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A6495	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A6497	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A6493	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A6494	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A6495	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A6497	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096	FIPS 186-4

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

Algorithm	CAVP Cert	Properties	Reference
		Primality Tests - Table C.2 Private Key Format - Standard	
RSA KeyGen (FIPS186-5)	A6493	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6494	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6495	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6497	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-4)	A6493	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A6494	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A6495	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A6497	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-5)	A6493	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigGen (FIPS186-5)	A6494	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigGen (FIPS186-5)	A6495	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigGen (FIPS186-5)	A6497	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A6493	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6494	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6495	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6497	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A6493	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5

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

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A6494	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6495	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6497	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
Safe Primes Key Generation	A6497	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6500	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
SHA2-512	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6493	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6494	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6495	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA3-224	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-224	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-256	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-256	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A6497	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A6500	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHAKE-128	A6500	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A6500	Output Length - Output Length: 16-65536 Increment 8	FIPS 202

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

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

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

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

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

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

Non-Approved, Not Allowed Algorithms:

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

Name	Use and Function
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
Diffie-Hellman	Shared Secret Computation using key size < 2048
ECDSA	PKG: Curve P-192; PKV: Curve P-192; compact point representation of points; Signature Generation: Curve P-192; Signature Verification: Curve P-192
EC Diffie-Hellman	Shared Secret Computation using curves < P-224
Ed25519	Key Generation, Signature Generation, Signature Verification, X25519 Key Agreement
Integrated Encryption Scheme on elliptic curves	Encryption/Decryption
MD2	Message Digest size: 128-bit
MD4	Message Digest size: 128-bit
MD5	Message Digest size: 160-bit (except in the TLS 1.0/1.1 context)
OMAC (One-Key CBC MAC)	MAC Generation
RC2	Encryption/Decryption Key Sizes 8 to 1024-bits
RC4	Encryption/Decryption Key Sizes 8 to 4096-bits
RFC6637	Key Derivation Function
RIPEMD	Message Digest size: 160-bits
RSA Keygen	ANSI X9.31 Key Pair Generation; keys < 2048-bits
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/Decryption; CBC, CTR, CFB64, ECB, CFB8, OFB
HPKE (Hybrid Public Key Encryption) [RFC9180]	Hybrid encryption scheme

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

Table 9: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

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

Name	Type	Description	Properties	Algorithms
AES Cipher	BC-UnAuth	AES Symmetric Encryption and Decryption		AES-ECB: (A6489, A6490, A6491, A6492, A6497, A6498, A6499) AES-CBC: (A6489, A6490, A6491, A6492, A6496, A6497) AES-CFB8: (A6491, A6492, A6497) AES-CFB128: (A6491, A6492, A6497) AES-CTR: (A6491, A6492, A6497, A6498, A6499) AES-OFB: (A6491, A6492, A6497) AES-XTS Testing Revision 2.0: (A6489, A6490, A6491, A6492, A6497)
AES Authenticated Cipher	BC-Auth	AES Authenticated Encryption and Decryption		AES-CCM: (A6491, A6492, A6497, A6498, A6499) AES-GCM: (A6491, A6492, A6497, A6498, A6499) AES-KW: (A6491, A6492, A6497)
MAC (CMAC)	MAC	CMAC Generation and Verification		AES-CMAC: (A6497)
MAC (HMAC)	MAC	HMAC Generation and Verification		HMAC-SHA-1: (A6493, A6494, A6495, A6497,

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

Name	Type	Description	Properties	Algorithms
				A6500) HMAC-SHA2-224: (A6493, A6494, A6495, A6497, A6500) HMAC-SHA2-256: (A6493, A6494, A6495, A6497, A6500) HMAC-SHA2-384: (A6493, A6494, A6495, A6497, A6500) HMAC-SHA2-512: (A6493, A6494, A6495, A6497, A6500) HMAC-SHA2-512/256: (A6493, A6494, A6495, A6497) HMAC-SHA3-224: (A6497, A6500) HMAC-SHA3-256: (A6497, A6500) HMAC-SHA3-384: (A6497, A6500) HMAC-SHA3-512: (A6497, A6500)
Message Digest	SHA	SHA Digest and MD5 Digest		SHA-1: (A6493, A6494, A6495, A6497, A6500) SHA2-224: (A6493, A6494, A6495, A6497, A6500) SHA2-256: (A6493, A6494, A6495, A6497, A6500) SHA2-384: (A6493, A6494, A6495, A6497, A6500) SHA2-512: (A6493, A6494,

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

Name	Type	Description	Properties	Algorithms
				A6495, A6497, A6500) SHA2-512/256: (A6493, A6494, A6495, A6497) SHA3-224: (A6497, A6500) SHA3-256: (A6497, A6500) SHA3-384: (A6497, A6500) SHA3-512: (A6497, A6500) MD5: ()
Message Digest (XOF)	XOF	XOF Digest		SHAKE-128: (A6500) SHAKE-256: (A6500)
Key Derivation	KAS-56CKDF KBKDF PBKDF	Key Derivation		KDA HKDF SP800-56Cr2: (A6493, A6494, A6495, A6497, A6500) KDF SP800-108: (A6493, A6494, A6495, A6497) PBKDF: (A6493, A6494, A6495, A6497)
Random Bit Generation	DRBG	Random Bit Generation		Counter DRBG: (A6491, A6492, A6497, A6498, A6499) HMAC DRBG: (A6493, A6494, A6495, A6497)
ECC Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer CKG	ECDSA Asymmetric Key Pair Generation and Verification		ECDSA KeyGen (FIPS186-4): (A6493, A6494, A6495, A6497) ECDSA KeyVer (FIPS186-4): (A6493, A6494, A6495, A6497) ECDSA KeyGen (FIPS186-5): (A6493, A6494, A6495, A6497)

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

Name	Type	Description	Properties	Algorithms
				ECDSA KeyVer (FIPS186-5): (A6493, A6494, A6495, A6497) CKG: () Key Type: Asymmetric
FFC Key Generation	AsymKeyPair-KeyGen CKG	Safe Primes Key Generation		Safe Primes Key Generation: (A6497) CKG: () Key Type: Asymmetric
IFC Key Generation	AsymKeyPair-KeyGen CKG	RSA Asymmetric Key Pair Generation		RSA KeyGen (FIPS186-4): (A6493, A6494, A6495, A6497) RSA KeyGen (FIPS186-5): (A6493, A6494, A6495, A6497) CKG: () Key Type: Asymmetric
ECDSA Digital Signature	DigSig-SigGen DigSig-SigVer	ECDSA Digital Signature Generation and Verification		ECDSA SigGen (FIPS186-4): (A6493, A6494, A6495, A6497) ECDSA SigVer (FIPS186-4): (A6493, A6494, A6495, A6497) ECDSA SigGen (FIPS186-5): (A6493, A6494, A6495, A6497) ECDSA SigVer (FIPS186-5): (A6493, A6494, A6495, A6497)
RSA Digital Signature	DigSig-SigGen DigSig-SigVer	RSA Digital Signature Generation and Verification		RSA SigGen (FIPS186-4): (A6493, A6494, A6495, A6497) RSA SigVer (FIPS186-4): (A6493, A6494, A6495, A6497) RSA SigGen

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

Name	Type	Description	Properties	Algorithms
				(FIPS186-5): (A6493, A6494, A6495, A6497) RSA SigVer (FIPS186-5): (A6493, A6494, A6495, A6497)
ECC Key Agreement	KAS-SSC	ECC Key Agreement. Scheme: EphemeralUnified, KAS Role: Initiator, Responder	SP800-56Ar3 KAS-ECC-SSC per IG D.F Scenario 2 path (1):P-224, P-256, P-384, P-521 curves providing 112, 128, 192, or 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6497)
FFC Key Agreement	KAS-SSC	FFC Key Agreement. Scheme: dhEphem: KAS Role: initiator, responder	SP800-56Ar3 KAS-FFC-SSC IG D.F Scenario 2 path (1):2048, 3072, 4096, 6144, and 8192-bit key providing 112, 128, 152, 176, or 200 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A6497)

Table 10: Security Function Implementations

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

2.7 Algorithm Specific Information

GCM IV

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

The GCM IV generation follows RFC 5288 shall only be used for the TLS protocol version 1.2. This implementation is compatible with acceptable AES-GCM cipher suites from SP800-52r2 Section 3.3.1. The IV consists of 12 bytes (96 bits) divided into two fields: the salt (fixed field), which is 4 bytes (32 bits), and the explicit nonce (counter field), which is 8 bytes (64 bits). The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the *nonce_explicit*, or counter portion of the IV will not exhaust all of its possible values.

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

The GCM IV generation follows RFC 4106 and shall only be used for the IPsec-v3 protocol version 3. The IV consists of 12 bytes (96 bits) divided into two fields: the salt (fixed field), which is 4 bytes (32 bits), and the counter portion, which is 8 bytes (64 bits). The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the IPsec protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the IPsec protocol implicitly ensures that the *nonce_explicit*, or counter portion of the IV will not exhaust all of its possible values.

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

AES-XTS

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

Key Derivation using SP 800-132 PBKDF2

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

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.

Key Agreement (KAS)

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

2.8 RBG and Entropy

The tables below detail the modules ESV information.

Cert Number	Vendor Name
E14	apple
E264	apple

Table 11: Entropy Certificates

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

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 Sequoia 15 on Intel Coffee Lake 9th Gen Intel(R) Core(TM) i9-9880H; macOS Sequoia 15 on Intel Comet Lake 10th Gen Intel(R) Core(TM) i9-10910; macOS Sequoia 15 on Intel Cascade Lake Intel(R) Xeon(R) W-3223; macOS Sequoia 15 on Intel Skylake Intel(R) Xeon(R) W-2140B	512 bits	512 bits	SHA2-512 [ACVP Cert #A6400]

Table 12: Entropy Sources

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

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

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

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

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

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

2.9 Key Generation

The module generates Keys and SSPs in accordance with FIPS 140-3 IG D.H. The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP 800-133r2] Section 4, Example 1 (vendor affirmed), compliant with [FIPS186-4] and [FIPS186-5], and using DRBG compliant with [SP 800-90Ar1]. A seed (the random value) used in asymmetric key generation is obtained from [SP 800-90Ar1] DRBG. The key generation service for RSA, Diffie-Hellman and EC key pairs as well as the [SP 800-90Ar1] DRBG have been ACVT tested with algorithm certificates.

The module also implements the following key derivation functions:

- KDA HKDF Key Derivation according to [SP 800-56Cr1] to derive symmetric keys. The module supports HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, or HMAC-SHA3-512 as the pseudo-random function (PRF).
- KBKDF Key Derivation according to [SP 800-108r1] to derive symmetric keys. The module supports Counter mode with AES-CMAC (128, 192, 256 bits), HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384,

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

HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, or HMAC-SHA3-512 as the pseudo-random function (PRF).

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

2.10 Key Establishment

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

- Diffie-Hellman Shared Secret Computation

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

- EC Diffie-Hellman Shared Secret Computation

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

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

2.11 Industry Protocols

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

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

Table 13: Ports and Interfaces

The module does not implement a Control Output Logical Interface.

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 14: Roles

4.3 Approved Services

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

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
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 Message Digest (XOF)	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
Message Authentication Generation	Generate a MAC digest using the requested SHA algorithm or AES algorithm	0	Message, MAC key, MAC algorithm	MAC	MAC (CMAC) MAC (HMAC)	Crypto Officer - AES Key: W,E - HMAC Key: W,E
Message Authentication Verification	Verify a MAC digest	0	MAC, message, MAC key, MAC algorithm	Pass/Fail	MAC (CMAC) MAC (HMAC)	Crypto Officer - AES Key: W,E - 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
PBKDF	Derive key from password	0	Password	PBKDF derived key	Key Derivation	Crypto Officer - PBKDF Password: W,E - PBKDF 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

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
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 - ECDSA Private Key: G,R - ECDSA Public Key: G,R
RSA Key Pair Generation	Generate a keypair for a requested modulus	0	Key size	RSA Key pair	IFC Key Generation	Crypto Officer - DRBG Seed, Internal State V, and Key (IG D.L): E - RSA Private Key: G,R - RSA Public Key: G,R
Safe Primes Key Generation	Generate a keypair for a requested 'safe' domain parameter	0	Key size	FFC Key pair	FFC Key Generation	Crypto Officer - DRBG Seed, Internal State V, and Key (IG D.L): E - Diffie-Hellman Private Key: G,R - Diffie-Hellman Public Key: G,R

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
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
Diffie-Hellman Shared Secret Computation	Generate a shared secret	0	Domain parameter, received public key and possessed private key	Shared secret	FFC Key Agreement	Crypto Officer - Diffie-Hellman Private Key: W,E - Diffie-Hellman Public Key: W,E
EC Diffie-Hellman Shared Secret Computation	Generate a shared secret	0	Domain parameter, received public key and	Shared secret	ECC Key Agreement	Crypto Officer - EC Diffie-Hellman Private

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			possessed private key			Key: W,E - EC Diffie-Hellman Public Key: W,E
On-Demand Self-test	Execute on-demand self-tests	N/A	N/A	Pass or Fail	AES Cipher AES Authenticated Cipher MAC (CMAC) MAC (HMAC) Message Digest Message Digest (XOF) Key Derivation Random Bit Generation ECC Key Generation FFC Key Generation IFC Key Generation ECDSA Digital Signature RSA Digital Signature ECC Key Agreement FFC Key Agreement	Crypto Officer
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	N/A	N/A	Module information	None	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
	Version Number					
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 - PBKDF Password: Z - PBKDF Derived Key: Z - Entropy Input String: Z - 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 - Diffie-Hellman

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - Diffie-Hellman Public Key: Z - EC Diffie-Hellman Private Key: Z - EC Diffie-Hellman Public Key: Z

Table 15: Approved Services

4.4 Non-Approved Services

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

Name	Description	Algorithms	Role
ANSI X9.63 KDF	Hash based Key Derivation Function	ANSI X9.63 KDF	CO
Blowfish	Encryption and Decryption	Blowfish	CO
CAST5	Encryption and Decryption, Key Sizes: 40 to 128 bits in 8-bit increments	CAST5	CO
DES	Encryption and Decryption, Key Size: 56-bits	DES	CO
Diffie-Hellman	Shared Secret Computation using key size < 2048	Diffie-Hellman	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
EC Diffie-Hellman	Shared Secret Computation using curves < P-224	EC Diffie-Hellman	CO
Ed25519	Key Generation, Signature Generation, Signature Verification, X25519 Key Agreement	Ed25519	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 (except in the TLS 1.0/1.1 context)	MD5	CO
OMAC (One-Key CBC MAC)	MAC Generation	OMAC (One-Key CBC MAC)	CO

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

Name	Description	Algorithms	Role
RC2	Encryption and Decryption, Key Sizes 8 to 1024-bits	RC2	CO
RC4	Encryption and Decryption, Key Sizes 8 to 4096-bits	RC4	CO
RFC6637	Key Derivation Function	RFC6637	CO
RIPEMD	Message Digest size: 160-bits	RIPEMD	CO
RSA Keygen	ANSI X9.31 Key Pair Generation; keys < 2048-bits	RSA Keygen	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/Decryption; CBC, CTR, CFB64, ECB, CFB8, OFB	Triple-DES [SP 800-67]	CO
HPKE (Hybrid Public Key Encryption)	Hybrid Encryption Scheme	HPKE (Hybrid Public Key Encryption) [RFC9180]	CO

Table 16: 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 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 Host OS, 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 v18.3 [Intel, User, 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 17: Storage Areas

9.2 SSP Input-Output Methods

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

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

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

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

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

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

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

Table 19: SSP Zeroization Methods

9.4 SSPs

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Cipher AES Authenticated Cipher MAC (CMAC)
AES Key-Wrapping Key	AES-KW key	128 to 256 bits - 128 to 256 bits	Symmetric Key - CSP			AES Authenticated Cipher
HMAC Key	HMAC key	2 to 262144 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		
PBKDF Password	PBKDF input password	64 to 1024 bits - N/A	Password - CSP			Key Derivation
PBKDF Derived Key	PBKDF 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

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
DRBG Seed, Internal State V, and Key (IG D.L)	DRBG input parameters	256 bits - 256 bits	DRBG parameters - CSP	Random Bit Generation		Random Bit Generation
ECDSA 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 (including intermediate keygen values)	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - CSP	IFC Key Generation		RSA Digital Signature
RSA Public Key	RSA public key (including intermediate keygen values)	2048 to 4096 bits - 112 to 150 bits	Asymmetric Key - PSP	IFC Key Generation		RSA Digital Signature
Diffie-Hellman Private Key	Diffie-Hellman private key (including intermediate keygen values)	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits	Asymmetric Key - CSP	FFC Key Generation		FFC Key Agreement
Diffie-Hellman Public Key	Diffie-Hellman public key (including intermediat	MODP-2048, MODP-3072, MODP-	Asymmetric Key - PSP	FFC Key Generation		FFC Key Agreement

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)	4096, MODP-6144, MODP-8192 - 112 to 200 bits				
EC Diffie-Hellman Private Key	EC Diffie-Hellman private key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - CSP	ECC Key Generation		ECC Key Agreement
EC Diffie-Hellman Public Key	EC Diffie-Hellman public key (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric Key - PSP	ECC Key Generation		ECC Key Agreement

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	
AES Key-Wrapping Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	
HMAC Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	
KDF Key Derivation Key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KDF Derived Key:Derives

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
KDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KDF Key Derivation Key:Derived From
PBKDF Password	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF Derived Key:Derives
PBKDF Derived Key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF Password:Derived From
Entropy Input String	API input parameters	RAM:Plaintext	From service invocation to service completion	Power down	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	Power down	Entropy Input String:Generated From
ECDSA Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	ECDSA Public Key:Paired With
ECDSA Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	ECDSA Private Key:Paired With
RSA Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	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
RSA Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	RSA Private Key:Paired With
Diffie-Hellman Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	Diffie-Hellman Public Key:Paired With
Diffie-Hellman Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	Diffie-Hellman Private Key:Paired With
EC Diffie-Hellman Private Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	EC Diffie-Hellman Public Key:Paired With
EC Diffie-Hellman Public Key	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	EC Diffie-Hellman Private Key:Paired With

Table 21: 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.

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.

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 (A6500)	112-bit key	Message Authentication over the complete module file image	SW/FW Integrity	Module successful execution	The HMAC-SHA2-256 value calculated at runtime is compared with the HMAC-SHA2-256 value stored in the module, computed at compilation time

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A6491) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-GCM (A6491) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-GCM (A6492) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-GCM (A6492) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-GCM (A6497) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on

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
						after the integrity test
AES-GCM (A6497) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-GCM (A6498) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-GCM (A6498) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-GCM (A6499) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-GCM (A6499) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-CCM (A6491) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-CCM (A6491) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-CCM (A6492) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-CCM (A6492) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-CCM (A6497) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-CCM (A6497) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	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
AES-CCM (A6498) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-CCM (A6498) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
AES-CCM (A6499) encrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Encryption	Test runs at power-on after the integrity test
AES-CCM (A6499) decrypt	128-bit key	KAT	CAST	Module becomes operational	Authenticated Decryption	Test runs at power-on after the integrity test
Counter DRBG (A6491)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
Counter DRBG (A6492)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
Counter DRBG (A6497)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
Counter DRBG (A6498)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
Counter DRBG (A6499)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	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 (A6493)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
HMAC DRBG (A6494)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
HMAC DRBG (A6495)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
HMAC DRBG (A6497)	As specified in NIST SP 800-90Ar1	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6493)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6494)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6495)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6497)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA-1 (A6500)	SHA-1	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6493)	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 (A6494)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6495)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6497)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-256 (A6500)	SHA2-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A6493)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6494)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6495)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6497)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512 (A6500)	SHA2-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6493)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6494)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA2-512/256 (A6495)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	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
HMAC-SHA2-512/256 (A6497)	SHA2-512/256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-224 (A6497)	SHA3-224	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-224 (A6500)	SHA3-224	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-256 (A6497)	SHA3-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-256 (A6500)	SHA3-256	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-384 (A6497)	SHA3-384	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-384 (A6500)	SHA3-384	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-512 (A6497)	SHA3-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
HMAC-SHA3-512 (A6500)	SHA3-512	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
AES-CMAC (A6497)	128-bit key	KAT	CAST	Module becomes operational	Message Authentication	Test runs at power-on after the integrity test
RSA KeyGen (FIPS186-4) (A6493)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A6494)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

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
RSA KeyGen (FIPS186-4) (A6495)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-4) (A6497)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA SigGen (FIPS186-4) (A6493)	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) (A6494)	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) (A6495)	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) (A6497)	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) (A6493)	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) (A6494)	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) (A6495)	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) (A6497)	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 KeyGen (FIPS186-5) (A6493)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-5) (A6494)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

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
RSA KeyGen (FIPS186-5) (A6495)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA KeyGen (FIPS186-5) (A6497)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
RSA SigGen (FIPS186-5) (A6493)	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 (FIPS186-5) (A6494)	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 (FIPS186-5) (A6495)	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 (FIPS186-5) (A6497)	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 (FIPS186-5) (A6493)	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 (FIPS186-5) (A6494)	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 (FIPS186-5) (A6495)	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 (FIPS186-5) (A6497)	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) (A6493)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A6494)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

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
ECDSA KeyGen (FIPS186-4) (A6495)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-4) (A6497)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA SigGen (FIPS186-4) (A6493)	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) (A6494)	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) (A6495)	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) (A6497)	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) (A6493)	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) (A6494)	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) (A6495)	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) (A6497)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA KeyGen (FIPS186-5) (A6493)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6494)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation

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
ECDSA KeyGen (FIPS186-5) (A6495)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA KeyGen (FIPS186-5) (A6497)	PCT	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
ECDSA SigGen (FIPS186-5) (A6493)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-5) (A6494)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-5) (A6495)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigGen (FIPS186-5) (A6497)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Generation	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-5) (A6493)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-5) (A6494)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-5) (A6495)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
ECDSA SigVer (FIPS186-5) (A6497)	P-224 with SHA2-224	KAT	CAST	Module becomes operational	Digital Signature Verification	Test runs at power-on after the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A6497)	P-224	KAT	CAST	Module becomes operational	Shared Secret Computation	Test runs at power-on after the integrity test
KAS-FFC-SSC Sp800-	MODP-2048	KAT	CAST	Module becomes operational	Shared Secret Computation	Test runs at power-on

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
56Ar3 (A6497)						after the integrity test
Safe Primes Key Generation (A6497)	MODP-2048	PCT	PCT	Successful key pair generation	Key Generation	Key pair generation
KDA HKDF SP800-56Cr2 (A6493)	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
KDA HKDF SP800-56Cr2 (A6494)	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
KDA HKDF SP800-56Cr2 (A6495)	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
KDA HKDF SP800-56Cr2 (A6497)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
KDA HKDF SP800-56Cr2 (A6500)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
KDF SP800-108 (A6493)	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
KDF SP800-108 (A6494)	Counter mode KDF with HMAC-SHA-1, HMAC-SHA2-	KAT	CAST	Module becomes operational	Key Derivation	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
	256, HMAC-SHA2-512					
KDF SP800-108 (A6495)	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
KDF SP800-108 (A6497)	Counter mode KDF with CMAC-AES-128, CMAC-AES-256, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A6493)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A6494)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A6495)	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at power-on after the integrity test
PBKDF (A6497)	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
AES-CBC (A6489) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6489) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-CBC (A6490) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6490) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on

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
						after the integrity test
AES-CBC (A6491) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6491) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-CBC (A6492) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6492) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-CBC (A6496) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6496) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-CBC (A6497) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-CBC (A6497) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6489) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6489) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6490) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	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
AES-ECB (A6490) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6491) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6491) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6492) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6492) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6497) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6497) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6498) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6498) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-ECB (A6499) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-ECB (A6499) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	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
2.0 (A6189) encrypt						
AES-XTS Testing Revision 2.0 (A6189) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6490) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6490) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6491) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6491) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6492) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6492) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6497) encrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Encryption	Test runs at power-on after the integrity test
AES-XTS Testing Revision 2.0 (A6497) decrypt	128-bit key	KAT	CAST	Module becomes operational	Symmetric Decryption	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
SHAKE-128 (A6500)	SHAKE-128	KAT	CAST	Module becomes operational	XOF	Test runs at power-on after the integrity test
SHAKE-256 (A6500)	SHAKE-256	KAT	CAST	Module becomes operational	XOF	Test runs at power-on after the integrity test

Table 23: Conditional Self-Tests

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

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

10.3 Periodic Self-Test Information

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

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A6500)	Message Authentication over the complete module file image	SW/FW Integrity	Whenever module is powered on	Upon every power on

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A6491) encrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6491) decrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6492) encrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6492) decrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6497) encrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6497) decrypt	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-GCM (A6498) encrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6498) decrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6499) encrypt	KAT	CAST	On Demand	Power cycle
AES-GCM (A6499) decrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6491) encrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6491) decrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6492) encrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6492) decrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6497) encrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6497) decrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6498) encrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6498) decrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6499) encrypt	KAT	CAST	On Demand	Power cycle
AES-CCM (A6499) decrypt	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6491)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6492)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6497)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6498)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A6499)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6493)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6494)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6495)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6493)	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
HMAC-SHA-1 (A6494)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6495)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA-1 (A6500)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6493)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6494)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6495)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (A6500)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6493)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6494)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6495)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512 (A6500)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6493)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6494)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6495)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-512/256 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-224 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-224 (A6500)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-256 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-256 (A6500)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-384 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-384 (A6500)	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
HMAC-SHA3-512 (A6497)	KAT	CAST	On Demand	Power cycle
HMAC-SHA3-512 (A6500)	KAT	CAST	On Demand	Power cycle
AES-CMAC (A6497)	KAT	CAST	On Demand	Power cycle
RSA KeyGen (FIPS186-4) (A6493)	PCT	PCT	On Demand	Power cycle
RSA KeyGen (FIPS186-4) (A6494)	PCT	PCT	On Demand	Power cycle
RSA KeyGen (FIPS186-4) (A6495)	PCT	PCT	On Demand	Power cycle
RSA KeyGen (FIPS186-4) (A6497)	PCT	PCT	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6493)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6494)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6495)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-4) (A6497)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6493)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6494)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6495)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A6497)	KAT	CAST	On Demand	Power cycle
RSA KeyGen (FIPS186-5) (A6493)	PCT	PCT	On Demand	Power cycle
RSA KeyGen (FIPS186-5) (A6494)	PCT	PCT	On Demand	Power cycle

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 KeyGen (FIPS186-5) (A6495)	PCT	PCT	On Demand	Power cycle
RSA KeyGen (FIPS186-5) (A6497)	PCT	PCT	On Demand	Power cycle
RSA SigGen (FIPS186-5) (A6493)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-5) (A6494)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-5) (A6495)	KAT	CAST	On Demand	Power cycle
RSA SigGen (FIPS186-5) (A6497)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-5) (A6493)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-5) (A6494)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-5) (A6495)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-5) (A6497)	KAT	CAST	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6493)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6494)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6495)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-4) (A6497)	PCT	PCT	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A6493)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A6494)	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
ECDSA SigGen (FIPS186-4) (A6495)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-4) (A6497)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6493)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6494)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6495)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-4) (A6497)	KAT	CAST	On Demand	Power cycle
ECDSA KeyGen (FIPS186-5) (A6493)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-5) (A6494)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-5) (A6495)	PCT	PCT	On Demand	Power cycle
ECDSA KeyGen (FIPS186-5) (A6497)	PCT	PCT	On Demand	Power cycle
ECDSA SigGen (FIPS186-5) (A6493)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-5) (A6494)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-5) (A6495)	KAT	CAST	On Demand	Power cycle
ECDSA SigGen (FIPS186-5) (A6497)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-5) (A6493)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-5) (A6494)	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
ECDSA SigVer (FIPS186-5) (A6495)	KAT	CAST	On Demand	Power cycle
ECDSA SigVer (FIPS186-5) (A6497)	KAT	CAST	On Demand	Power cycle
KAS-ECC-SSC Sp800-56Ar3 (A6497)	KAT	CAST	On Demand	Power cycle
KAS-FFC-SSC Sp800-56Ar3 (A6497)	KAT	CAST	On Demand	Power cycle
Safe Primes Key Generation (A6497)	PCT	PCT	On Demand	Power cycle
KDA HKDF SP800-56Cr2 (A6493)	KAT	CAST	On Demand	Power cycle
KDA HKDF SP800-56Cr2 (A6494)	KAT	CAST	On Demand	Power cycle
KDA HKDF SP800-56Cr2 (A6495)	KAT	CAST	On Demand	Power cycle
KDA HKDF SP800-56Cr2 (A6497)	KAT	CAST	On Demand	Power cycle
KDA HKDF SP800-56Cr2 (A6500)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A6493)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A6494)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A6495)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A6497)	KAT	CAST	On Demand	Power cycle
PBKDF (A6493)	KAT	CAST	On Demand	Power cycle
PBKDF (A6494)	KAT	CAST	On Demand	Power cycle
PBKDF (A6495)	KAT	CAST	On Demand	Power cycle
PBKDF (A6497)	KAT	CAST	On Demand	Power cycle
AES-CBC (A6489) encrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6489) decrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6490) encrypt	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-CBC (A6490) decrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6491) encrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6491) decrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6492) encrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6492) decrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6496) encrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6496) decrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6497) encrypt	KAT	CAST	On Demand	Power cycle
AES-CBC (A6497) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6489) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6489) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6490) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6490) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6491) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6491) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6492) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6492) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6497) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6497) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6498) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6498) decrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6499) encrypt	KAT	CAST	On Demand	Power cycle
AES-ECB (A6499) decrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision	KAT	CAST	On Demand	Power cycle

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

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
2.0 (A6189) encrypt				
AES-XTS Testing Revision 2.0 (A6189) decrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6490) encrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6490) decrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6491) encrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6491) decrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6492) encrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6492) decrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6497) encrypt	KAT	CAST	On Demand	Power cycle
AES-XTS Testing Revision 2.0 (A6497) decrypt	KAT	CAST	On Demand	Power cycle
SHAKE-128 (A6500)	KAT	CAST	On Demand	Power cycle
SHAKE-256 (A6500)	KAT	CAST	On Demand	Power cycle

Table 25: Conditional Periodic Information

10.4 Error States

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

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

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 and EC Diffie- Hellman Error code "CCRSA_GENERATE_KEY_CONSISTENCY" returned for RSA Error code "CCDH_GENERATE_KEY_CONSISTENCY" returned for Diffie-Hellman

Table 26: 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 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.
- PBKDF see Section 2.7.

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

11.5 End of Life

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

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.