Apple Inc.

Apple corecrypto Module 18.3 [Apple silicon, User, Software, SL1]

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

© 2025 Apple Inc., All rights reserved.

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

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 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 13
2.4 Modes of Operation 13
2.5 Algorithms 14
2.6 Security Function Implementations 22
2.7 Algorithm Specific Information 29
2.8 RBG and Entropy 30
2.9 Key Generation 31
2.10 Key Establishment 32
2.11 Industry Protocols 32
3 Cryptographic Module Interfaces 32
3.1 Ports and Interfaces 32
4 Roles, Services, and Authentication 33
4.1 Authentication Methods 33
4.2 Roles 33
4.3 Approved Services 33
4.4 Non-Approved Services 41
4.5 External Software/Firmware Loaded 42
5 Software/Firmware Security 43
5.1 Integrity Techniques 43
5.2 Initiate on Demand 43
6 Operational Environment 44
6.1 Operational Environment Type and Requirements 44

© 2025 Apple Inc., All rights reserved.

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

6.2 Configuration Settings and Restrictions ... 44
7 Physical Security ... 45
8 Non-Invasive Security ... 46
9 Sensitive Security Parameters Management ... 47
9.1 Storage Areas ... 47
9.2 SSP Input-Output Methods ... 47
9.3 SSP Zeroization Methods ... 47
9.4 SSPs ... 48
9.5 Transitions ... 53
10 Self-Tests ... 54
10.1 Pre-Operational Self-Tests ... 54
10.2 Conditional Self-Tests ... 54
10.3 Periodic Self-Test Information ... 57
10.4 Error States ... 59
10.5 Operator Initiation of Self-Tests ... 59
11 Life-Cycle Assurance ... 60
11.1 Installation, Initialization, and Startup Procedures ... 60
11.2 Administrator Guidance ... 60
11.3 Non-Administrator Guidance ... 60
11.4 Design and Rules ... 60
11.5 End of Life ... 61
12 Mitigation of Other Attacks ... 62

© 2025 Apple Inc., All rights reserved.

This document may be reproduced and distributed only in its original entirely 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 12
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 13
Table 5: Modes List and Description 13
Table 6: Approved Algorithms 21
Table 7: Vendor-Affirmed Algorithms 21
Table 8: Non-Approved, Allowed Algorithms with No Security Claimed 21
Table 9: Non-Approved, Not Allowed Algorithms 22
Table 10: Security Function Implementations 29
Table 11: Entropy Certificates 30
Table 12: Entropy Sources 31
Table 13: Ports and Interfaces 32
Table 14: Roles 33
Table 15: Approved Services 41
Table 16: Non-Approved Services 42
Table 17: Storage Areas 47
Table 18: SSP Input-Output Methods 47
Table 19: SSP Zeroization Methods 48
Table 20: SSP Table 1 51
Table 21: SSP Table 2 53
Table 22: Pre-Operational Self-Tests 54
Table 23: Conditional Self-Tests 57
Table 24: Pre-Operational Periodic Information 57
Table 25: Conditional Periodic Information 58
Table 26: Error States 59

List of Figures

Figure 1: Block Diagram 7

© 2025 Apple Inc., All rights reserved.

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

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for Apple corecrypto Module 18.3 [Apple silicon, User, Software, SL1] cryptographic module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for a Security Level 1 module.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing. The vendor reviewed the intermediate and final Security Policy and approved all of its content.

© 2025 Apple Inc., All rights reserved.

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:
The Apple corecrypto Module 18.3 [Apple silicon, User, Software, SL1] cryptographic module (hereafter referred to as "the module") provides implementations of low-level cryptographic primitives to the Device OS's (iOS, iPadOS, watchOS, tvOS, visionOS, MacOS) 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 Device OS user space and does not contain any terminating assertions or exceptions. It is implemented as a Device OS dynamically loadable library. After the library is loaded, its cryptographic functions are made available to the Device OS application.

Any internal error detected by the module is returned to the caller with an appropriate return code. The calling Device 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

Module Characteristics:

Cryptographic Boundary:
The module cryptographic boundary is delineated by the dotted green rectangle in the Figure 1. The module executes within the user space of the computing platforms and operating systems listed in the Tested Operational Environments Table section 2.2.

© 2025 Apple Inc., All rights reserved.

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

Tested Operational Environment's Physical Perimeter (TOEPP):
The physical perimeter is represented by the most exterior black line in the block diagram Figure 1. The cryptographic boundary represented by the dotted green line includes the corecrypto component which forms the module.

Common crypto acts as a wrapper layer located outside of the module boundary, that provides a common interface for component within the TOEPP to access the module.

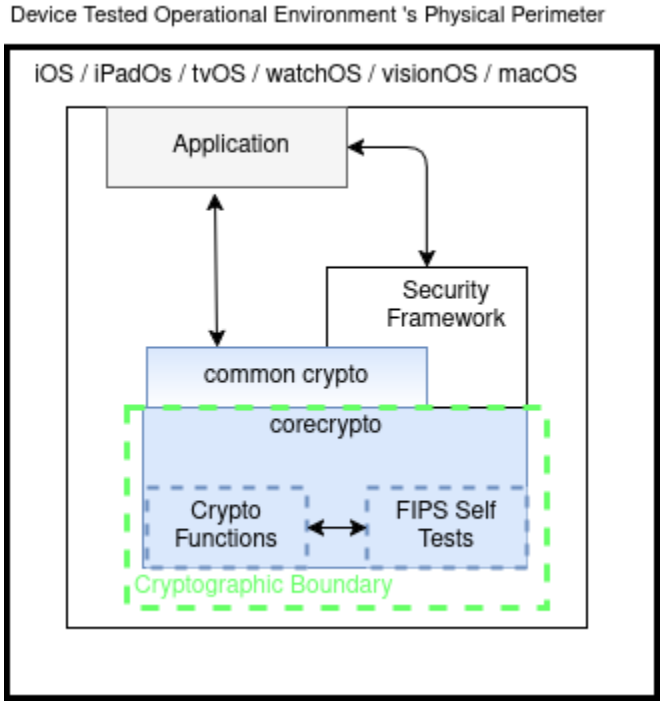

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

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

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
corecrypto-1736.80.2	18.3	N/A	HMAC-SHA256

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

© 2025 Apple Inc., All rights reserved.

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

© 2025 Apple Inc., All rights reserved.

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

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
iPadOS 18	iPad (9th generation)	Apple A Series A13 Bionic	Yes	NA	18.3
iPadOS 18	iPad (9th generation)	Apple A Series A13 Bionic	No	NA	18.3
iPadOS 18	iPad Air (4th generation)	Apple A Series A14 Bionic	Yes	NA	18.3
iPadOS 18	iPad Air (4th generation)	Apple A Series A14 Bionic	No	NA	18.3
iPadOS 18	iPad mini (6th generation)	Apple A Series A15 Bionic	Yes	NA	18.3
iPadOS 18	iPad mini (6th generation)	Apple A Series A15 Bionic	No	NA	18.3
iPadOS 18	iPad mini (7th generation)	Apple A Series A17 Pro	Yes	NA	18.3
iPadOS 18	iPad mini (7th generation)	Apple A Series A17 Pro	No	NA	18.3
iPadOS 18	iPad Pro 11-inch (3rd generation)	Apple M Series M1	Yes	NA	18.3
iPadOS 18	iPad Pro 11-inch (3rd generation)	Apple M Series M1	No	NA	18.3
iPadOS 18	iPad Pro 12.9-inch (6th generation)	Apple M Series M2	Yes	NA	18.3
iPadOS 18	iPad Pro 12.9-inch (6th generation)	Apple M Series M2	No	NA	18.3
iPadOS 18	iPad Pro 11-inch M4	Apple M Series M4	Yes	NA	18.3
iPadOS 18	iPad Pro 11-inch M4	Apple M Series M4	No	NA	18.3
iOS 18	iPhone 11 Pro Max	Apple A Series A13 Bionic	Yes	NA	18.3
iOS 18	iPhone 11 Pro Max	Apple A Series A13 Bionic	No	NA	18.3
iOS 18	iPhone 12	Apple A Series A14 Bionic	Yes	NA	18.3
iOS 18	iPhone 12	Apple A Series A14 Bionic	No	NA	18.3

© 2025 Apple Inc., All rights reserved.

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

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
iOS 18	iPhone 13 Pro Max	Apple A Series A15 Bionic	Yes	NA	18.3
iOS 18	iPhone 13 Pro Max	Apple A Series A15 Bionic	No	NA	18.3
iOS 18	iPhone 15 Plus	Apple A Series A16 Bionic	Yes	NA	18.3
iOS 18	iPhone 15 Plus	Apple A Series A16 Bionic	No	NA	18.3
iOS 18	iPhone 15 Pro Max	Apple A Series A17 Pro	Yes	NA	18.3
iOS 18	iPhone 15 Pro Max	Apple A Series A17 Pro	No	NA	18.3
iOS 18	iPhone 16	Apple A Series A18	Yes	NA	18.3
iOS 18	iPhone 16	Apple A Series A18	No	NA	18.3
iOS 18	iPhone 16 Pro	Apple A Series A18 Pro	Yes	NA	18.3
iOS 18	iPhone 16 Pro	Apple A Series A18 Pro	No	NA	18.3
watchOS 11	Apple Watch Series S9	Apple S Series S9	Yes	NA	18.3
watchOS 11	Apple Watch Series S9	Apple S Series S9	No	NA	18.3
watchOS 11	Apple Watch Series S10	Apple S Series S10	Yes	NA	18.3
watchOS 11	Apple Watch Series S10	Apple S Series S10	No	NA	18.3
tvOS 18	Apple TV 4K (3rd generation)	Apple A Series A15 Bionic	Yes	NA	18.3
tvOS 18	Apple TV 4K (3rd generation)	Apple A Series A15 Bionic	No	NA	18.3
macOS 15	MacBook Pro (13-inch, 2020)	Apple M Series M1	Yes	NA	18.3
macOS 15	MacBook Pro (13-inch, 2020)	Apple M Series M1	No	NA	18.3

© 2025 Apple Inc., All rights reserved.

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

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
macOS 15	MacBook Pro (16-inch, M1 Pro, 2021)	Apple M Series M1 Pro	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M1 Pro, 2021)	Apple M Series M1 Pro	No	NA	18.3
macOS 15	MacBook Pro (16-inch, M1 Max, 2021)	Apple M Series M1 Max	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M1 Max, 2021)	Apple M Series M1 Max	No	NA	18.3
macOS 15	Mac Studio	Apple M Series M1 Ultra	Yes	NA	18.3
macOS 15	Mac Studio	Apple M Series M1 Ultra	No	NA	18.3
macOS 15	MacBook Pro (13-inch, M2, 2020)	Apple M Series M2	Yes	NA	18.3
macOS 15	MacBook Pro (13-inch, M2, 2020)	Apple M Series M2	No	NA	18.3
macOS 15	MacBook Pro (16-inch, M2 Pro, 2023)	Apple M Series M2 Pro	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M2 Pro, 2023)	Apple M Series M2 Pro	No	NA	18.3
macOS 15	MacBook Pro (16-inch, M2 Max, 2023)	Apple M Series M2 Max	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M2 Max, 2023)	Apple M Series M2 Max	No	NA	18.3
macOS 15	Mac Studio (2023)	Apple M Series M2 Ultra	Yes	NA	18.3
macOS 15	Mac Studio (2023)	Apple M Series M2 Ultra	No	NA	18.3
macOS 15	MacBook Air (13-inch, 2024)	Apple M Series M3	Yes	NA	18.3
macOS 15	MacBook Air (13-inch, 2024)	Apple M Series M3	No	NA	18.3
macOS 15	MacBook Pro (14-inch, M3 Pro, Nov 2023)	Apple M Series M3 Pro	Yes	NA	18.3
macOS 15	MacBook Pro (14-inch, M3 Pro, Nov 2023)	Apple M Series M3 Pro	No	NA	18.3

© 2025 Apple Inc., All rights reserved.

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

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
macOS 15	MacBook Pro (14-inch, M3 Max, Nov 2023)	Apple M Series M3 Max	Yes	NA	18.3
macOS 15	MacBook Pro (14-inch, M3 Max, Nov 2023)	Apple M Series M3 Max	No	NA	18.3
macOS 15	Mac Mini (2024)	Apple M Series M4	Yes	NA	18.3
macOS 15	Mac Mini (2024)	Apple M Series M4	No	NA	18.3
macOS 15	MacBook Pro (16-inch, M4 Pro, 2024)	Apple M Series M4 Pro	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M4 Pro, 2024)	Apple M Series M4 Pro	No	NA	18.3
macOS 15	MacBook Pro (16-inch, M4 Max, 2024)	Apple M Series M4 Max	Yes	NA	18.3
macOS 15	MacBook Pro (16-inch, M4 Max, 2024)	Apple M Series M4 Max	No	NA	18.3
visionOS 2	Apple Vision Pro	Apple M Series M2	Yes	NA	18.3
visionOS 2	Apple Vision Pro	Apple M Series M2	No	NA	18.3

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

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

Operating System	Hardware Platform
iPadOS 18	iPad 7th gen with Apple A Series A10
iPadOS 18	iPad Air 3rd gen with Apple A Series A12 Bionic
iPadOS 18	iPad Mini 5th gen with Apple A Series A12 Bionic
iPadOS 18	iPad 8th gen with Apple A Series A12 Bionic
iPadOS 18	iPad Pro 12.9 in 3rd gen with Apple A Series A12X Bionic
iPadOS 18	iPad Pro 11 in 1st gen with Apple A Series A12X Bionic
iPadOS 18	iPad Pro 12.9 in 4th gen with Apple A Series A12Z Bionic
iPadOS 18	iPad Pro 11 in 2nd gen with Apple A Series A12Z Bionic
iOS 18	iPhone XR with Apple A Series A12 Bionic
iOS 18	iPhone XS with Apple A Series A12 Bionic
iOS 18	iPhone XS Max with Apple A Series A12 Bionic
tvOS 18	Apple TV 4K with Apple A Series A12 Bionic

© 2025 Apple Inc., All rights reserved.

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

Operating System	Hardware Platform
macOS 15	Apple Security Chip T2 with Apple T Series T2
watchOS 11	Apple Watch Series S6 with Apple S Series S6
watchOS 11	Apple Watch Series S7 with Apple S Series S7
watchOS 11	Apple Watch Series S8 with Apple S Series S8

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

None for this module.

2.4 Modes of Operation

Modes List and Description:

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 Table Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.	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

© 2025 Apple Inc., All rights reserved.

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

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:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6507	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6509	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A6508	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6510	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A6511	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A6507	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A6510	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6511	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A6507	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A6511	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6508	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6510	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A6511	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KW	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A6507	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A6508	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A6510	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A6507	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6508	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6510	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A6508	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6510	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A6511	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6510	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6512	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6510	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6512	Curve - P-224, P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6510	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
ECDSA SigGen (FIPS186-5)	A6512	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
ECDSA SigVer (FIPS186-4)	A6510	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 (FIPS186-4)	A6512	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)	A6510	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384,	FIPS 186-5

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
		SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	
ECDSA SigVer (FIPS186-5)	A6512	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-SHA-1	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6513	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6513	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6513	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A6513	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-224	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA3-224	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6510	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A6512	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6510	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	A6510	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	A6510	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
KDA HKDF SP800-56Cr2	A6512	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
KDA HKDF SP800-56Cr2	A6513	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-	SP 800-56C Rev. 2

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
		8192 Increment 8 HMAC Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA2-512/256	
KDF SP800-108	A6510	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
KDF SP800-108	A6512	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
PBKDF	A6510	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A6512	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-5)	A6510	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6512	Key Generation Mode - probableWithProbableAux Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6510	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigGen (FIPS186-5)	A6512	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-4)	A6510	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A6512	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-5)	A6510	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6512	Modulo - 2048, 3072, 4096 Signature Type - pss	FIPS 186-5
Safe Primes Key Generation	A6510	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A6513	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A6513	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A6513	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A6513	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA3-224	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-224	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-256	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 202

© 2025 Apple Inc., All rights reserved.

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

Algorithm	CAVP Cert	Properties	Reference
SHA3-256	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A6510	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A6512	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHAKE-128	A6512	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A6512	Output Length - Output Length: 16-65536 Increment 8	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric Implementations:c_ltc, vng_ltc	N/A	SP800-133rev2 section 4 example 1

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

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 KDF v1.0, v1.1 only)

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

Non-Approved, Not Allowed Algorithms:

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

© 2025 Apple Inc., All rights reserved.

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

Name	Use and Function
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
EdDSA with Ed25519	Key Generation, Signature Generation, Signature Verification
X25519 Key Agreement	Key agreement on X25519 curve
Integrated Encryption Scheme on elliptic curves	Encryption / Decryption
MD2	Message Digest size: 128-bit
MD4	Message Digest size: 128-bit
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	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]	Encrypt/Decrypt; CBC, CTR, CFB64, ECB, CFB8, OFB
HPKE (Hybrid Public Key Encryption) [RFC9180]	Hybrid encryption scheme
ML-KEM	Key Encapsulation
Keccak	Message Digest

Table 9: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption and Decryption	BC-UnAuth BC-Auth	Symmetric Encryption and Decryption	AES-CBC:Key Size / Key Strength: 128, 192, 256 bits AES-CFB128:Key Size / Key Strength: 128, 192, 256 bits	AES-CBC: (A6507, A6508, A6509, A6510) AES-CFB128: (A6507, A6508, A6510) AES-ECB: (A6507, A6508, A6510,

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
			AES-ECB:Key Size / Key Strength: 128, 192, 256 bits AES-OFB:Key Size / Key Strength: 128, 192, 256 bits AES-XTS Testing Revision 2.0:Key Size/ Key Strength: 128, 256 bits AES-CCM:Key Size / Key Strength: 128, 192, 256 bits AES-CFB8:Key Size / Key Strength: 128, 192, 256 bits AES-CTR:Key Size / Key Strength: 128, 192, 256 bits AES-GCM:Key Size / Key Strength: 128, 192, 256 bits	A6511) AES-OFB: (A6507, A6508, A6510) AES-XTS Testing Revision 2.0: (A6507, A6508, A6510) AES-CCM: (A6508, A6510, A6511) AES-CFB8: (A6508, A6510) AES-CTR: (A6508, A6510, A6511) AES-GCM: (A6508, A6510, A6511)
Key Wrapping	KTS-Wrap BC-Auth	Key Wrapping	Standard:SP 800-38F IG D.G:approved Caveat:Key establishment provides between 128 and 256 bits of security strength	AES-KW: (A6508, A6510)

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
Random Number Generation	DRBG	Random Number Generation	Counter DRBG:Key Size/ Key Strength: 128, 256 bits	Counter DRBG: (A6508, A6510, A6511)
Message authentication (MAC)	MAC	Message authentication (MAC)	AES-CMAC:Key Size / Key Strength: 128, 192, 256 bits HMAC-SHA-1:Key Size: 128 - 262144 bits; Key Strength: 128 bits HMAC-SHA2-224:Key Size: 224 - 262144 bits; Key Strength: 224 bits HMAC-SHA2-256:Key Size: 256 - 262144 bits; Key Strength: 256 bits HMAC-SHA2-384:Key Size: 384 - 262144 bits; Key Strength: 384 bits HMAC-SHA2-512:Key Size: 512 - 262144 bits; Key Strength: 512 bits HMAC-SHA2-512/256:Key Size: 512 -	AES-CMAC: (A6510) HMAC-SHA-1: (A6510, A6512) HMAC-SHA2-224: (A6510, A6512) HMAC-SHA2-256: (A6510, A6512, A6513) HMAC-SHA2-384: (A6510, A6512, A6513) HMAC-SHA2-512: (A6510, A6512, A6513) HMAC-SHA2-512/256: (A6510, A6512, A6513) HMAC-SHA3-224: (A6510, A6512) HMAC-SHA3-256: (A6510, A6512) HMAC-SHA3-384: (A6510, A6512) HMAC-SHA3-512: (A6510, A6512)

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
			262144 bits; Key Strength: 256 bits HMAC-SHA3-224:Key Size: 224 - 262144 bits; Key Strength: 224 bits HMAC-SHA3-256:Key Size: 256 - 262144 bits; Key Strength: 256 bits HMAC-SHA3-384:Key Size: 384 - 262144 bits; Key Strength: 384 bits HMAC-SHA3-512:Key Size: 512 - 262144 bits; Key Strength: 512 bits	
Asymmetric Key Generation	AsymKeyPair-KeyGen	Asymmetric Key Generation	ECDSA KeyGen (FIPS186-5):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA KeyGen (FIPS186-5):Key Size: 2048, 3072, 4096 bits; Key Strength: from 112 to 150 bits	ECDSA KeyGen (FIPS186-5): (A6510, A6512) RSA KeyGen (FIPS186-5): (A6510, A6512) Safe Primes Key Generation: (A6510) CKG: () Key Type: Asymmetric

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
			Safe Primes Generation:Safe Prime Groups: MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192; Key Strength: from 112 to 256 bits	Implementations: c_ltc, vng_ltc
Asymmetric Key Validation	AsymKeyPair-KeyVer	Asymmetric Key Validation	ECDSA KeyVer (FIPS186-5):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits	ECDSA KeyVer (FIPS186-5): (A6510, A6512)
Digital Signature Generation	DigSig-SigGen	Digital Signature Generation	ECDSA SigGen (FIPS186-5):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA SigGen (FIPS186-5):Key Size: 2048, 3072, 4096 bits; Key Strength: from 112 to 150 bits	ECDSA SigGen (FIPS186-5): (A6510, A6512) RSA SigGen (FIPS186-5): (A6510, A6512)
Digital Signature Verification	DigSig-SigVer	Digital Signature Verification	ECDSA SigVer (FIPS186-5):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA SigVer (FIPS186-5):Key	ECDSA SigVer (FIPS186-5): (A6510, A6512) RSA SigVer (FIPS186-5): (A6510, A6512)

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
			Size: 2048, 3072, 4096 bits; Key Strength: from 128 to 150 bits	
Digital Signature Verification (Legacy)	DigSig-SigVer	Digital Signature Verification	IG:C.M Key Size:1024 bits Security Strength:112 bits Message Digest:SHA-1	ECDSA SigVer (FIPS186-4): (A6510, A6512) RSA SigVer (FIPS186-4): (A6510, A6512) SHA-1: (A6510, A6512)
Shared Secret Computation	KAS-SSC	Shared Secret Computation	KAS-ECC-SSC Sp800-56Ar3:Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits KAS-FFC-SSC Sp800-56Ar3:Key Size: 2048, 3072, 4096, 6144, 8192 bits; Key Strength: from 112 to 200 bits	KAS-ECC-SSC Sp800-56Ar3: (A6510) KAS-FFC-SSC Sp800-56Ar3: (A6510)
Key Derivation (KBKDF)	KBKDF	Key Derivation - SP800-108 KBKDF	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits Supported Lengths:8-4096 Increment 8 Fixed Data Order:Before Fixed Data Counter	KDF SP800-108: (A6510, A6512)

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
			Length:8, 16, 24, 32	
Key Derivation (PBKDF)	PBKDF	Key Derivation - SP800-132 PBKDF	PBKDF:Key Size: 112 - 4096; Key Strength: 128 - 256; Password length: 8- 128 bytes Increment 1; Salt Length: 128-4096 Increment 8; Iteration Count: 1000-100000 Increment 1	PBKDF: (A6510, A6512)
Key Derivation (HKDF)	KAS-56CKDF	Key Derivation - SP800-56Crev2 HKDF	KDA HKDF:Shared Secret Length: 224-8192 Increment 8; Derived Key Length: 2048	KDA HKDF SP800-56Cr2: (A6510, A6512, A6513)
Message Digest	SHA XOF	Message Digest	Hashes:SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512 XOFs:SHAKE-128, SHAKE-256	SHA-1: (A6510, A6512) SHA2-224: (A6510, A6512) SHA2-256: (A6510, A6512, A6513) SHA2-384: (A6510, A6512, A6513) SHA2-512: (A6510, A6512, A6513) SHA2-512/256: (A6510, A6512, A6513) SHA3-224: (A6510, A6512) SHA3-256:

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Description	Properties	Algorithms
				(A6510, A6512) SHA3-384: (A6510, A6512) SHA3-512: (A6510, A6512) SHAKE-128: (A6512) SHAKE-256: (A6512)

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

GCM IV

AES-GCM IV is constructed in compliance with IG C.H scenario 1 (TLS 1.2 and 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 ciphersuites from SP800-52r2 Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the nonce_explicit, or counter portion of the IV will not exhaust all of its possible values.

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

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

AES-XTS

AES-XTS mode is only approved for hardware storage applications. The length of the AES-XTS data unit does not exceed 2^{20} blocks. It is the responsibility of the Operator to ensure Key_1 and Key_2 are generated independently according to the rules for component symmetric keys from

© 2025 Apple Inc., All rights reserved.

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

NIST SP 800-133rev2, Section 6.3. In compliance with IG C.I, before using the keys in the XTS-Algorithm, the module includes an explicit check to verify that Key_1 ≠ Key_2.

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 salt input to PBKDFv2 is 128-bits in accordance with section 5.1 of SP800-132. As is recommended SP800-132, PBKDFv2 is implemented to support a minimum iteration count of 1000, and is extended to support up to 10,000 iterations. PBKDFv2 is implemented to support the option 1a specified in section 5.4 of SP800-132. The derived keys may only be used in storage applications.

RSA

In compliance with IG C.F, all the RSA modulus sizes used by the cryptographic module have been CAVP 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.

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.

SHA-1

SHA-1 is only approved when used in approved mode for message digest and signature verification. Digital signature generation using SHA-1 is non-approved and not allowed in approved services. The SHA-1 algorithm, as implemented by the module, will be non-approved for all purposes except signature verification, starting January 1, 2031.

Legacy Algorithms

Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M. The FIPS 186-4 implementation of RSA and ECDSA SigVer using 1024 bits key and SHA-1, is allowed for legacy use only.

2.8 RBG and Entropy

Cert Number	Vendor Name
E113	Apple Inc.

Table 11: Entropy Certificates

© 2025 Apple Inc., All rights reserved.

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

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Apple corecrypto physical entropy source	Physical	Apple A Series A13 Bionic, Apple A Series A14 Bionic, Apple A Series A15 Bionic, Apple A Series A16 Bionic, Apple A Series A17 Pro, Apple A Series A18, Apple A Series A18 Pro, Apple S Series S9, Apple S Series S10, Apple M Series M1, Apple M Series M1 Pro, Apple M Series M1 Max, Apple M Series M1 Ultra, Apple M Series M2, Apple M Series M2 Pro, Apple M Series M2 Max, Apple M Series M2 Ultra, Apple M Series M3, Apple M Series M3 Pro, Apple M Series M3 Max, Apple M Series M4, Apple M Series M4 Pro, Apple M Series M4 Max	256 bits	Full Entropy	SHA-256 [ACVP cert. #C1223]

Table 12: Entropy Sources

Entropy source: The module makes use of a physical entropy source listed in the above table, which is located within the physical perimeter of the module (TOEPP) but outside the cryptographic boundary of the module. The entropy source runs on all processors listed in the above table, which accounts for and operates on all tested Operating Environments listed in the section 2.2 above. The output of the entropy source provides full entropy to seed and reseed SP800-90Arev1 DRBG during initialization and reseeding respectively.

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

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

2.9 Key Generation

See vendor affirmed algorithms (CKG) in section 2.5. The module implements RSA, ECDSA, and Safe Prime Key Generation in compliance with SP800-133rev2 section 4 example 1 and IG D.H.

© 2025 Apple Inc., All rights reserved.

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

The module does not implement symmetric key generation.

2.10 Key Establishment

The module offers Key Agreement (shared secret computation) using SP800-56Ar3 KAS-ECC-SSC or KAS-FFC-SSC compliant with IG D.F scenario 2(1). 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.

To comply with the assurances found in Section 5.6.2 of SP 800-56A Rev. 3, the operator must use the module's approved key pair generation service (see Approved Services table in Section 4.3 Approved Services) to generate ephemeral Diffie-Hellman or EC Diffie-Hellman key pairs, or the key pairs must be obtained from another FIPS-validated module. As part of key pair generation service service, the module will internally perform the full public key validation of the generated public key. The module's shared secret computation service will internally perform the full public key validation of the peer public key, complying with Sections 5.6.2.2.1 and 5.6.2.2.2 of SP 800-56A Rev. 3.

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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.

© 2025 Apple Inc., All rights reserved.

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

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

FIPS 140-3 does not require an authentication mechanism for level 1 modules. Therefore, the module does not support an authentication mechanism for Crypto Officer. The Crypto Officer role is authorized to access all services provided by the module (see Table - Approved Services and Table - Non-Approved Services).

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 14: Roles

4.3 Approved Services

The module implements a dedicated API function to indicate if a requested service utilizes an approved security function. The approved service indicator utilizes one of two functions (fips_allowed and fips_allowed_mode) depending on the service in question. Calling fips_allowed_mode with any approved AES mode will return a zero to indicate it is an approved algorithm. Similarly, calling fips_allowed with any other approved algorithm will return zero. Calling either of these with an algorithm not listed in the Approved Algorithms Table will return a non-zero value, and as such indicates a non-approved service.

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 (or failure)	Symmetric Encryption and Decryption	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	wrapped key / unwrapped key (or failure)	Key Wrapping	Crypto Officer - AES key-wrapping key: W,E

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			key, AES key wrapping key			
Secure Hash Generation	Generate a digest for the requested algorithm	0	message	digest	Message Digest	Crypto Officer
Message Authentication Generation	Generate a MAC digest using the requested SHA algorithm or AES algorithm	0	message, MAC key, MAC algorithm	MAC	Message authentication (MAC)	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	Message authentication (MAC)	Crypto Officer - AES key: W,E - HMAC 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	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	Digital Signature Generation Digital Signature Verification Digital Signature Verification (Legacy)	Crypto Officer - RSA key pair: W,E

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	public key.					
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	Digital Signature Generation Digital Signature Verification	Crypto Officer - ECDSA key pair: W,E
Random Number Generation	Generate random number	0	requested number of bits	random bit-string	Random Number Generation	Crypto Officer - Entropy input string: W,E,Z - DRBG seed, internal state V value, and key (IG D.L compliant): G,W,E
PBKDF	Derive key from password	0	PBKDF Password	PBKDF derived key	Key Derivation (PBKDF)	Crypto Officer - PBKDF derived key: G,R - PBKDF

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						password: W,E
KBKDF	Derive key from key derivation key	0	KBKDF key derivation key	KBKDF derived key	Key Derivation (KBKDF)	Crypto Officer - KBKDF key derivation key: W,E - KBKDF derived key: G,R
RSA key pair generation	Generate a keypair for a requested modulus	0	key size	key pair	Random Number Generation Asymmetric Key Generation	Crypto Officer - DRBG seed, internal state V value, and key (IG D.L compliant): W,E - RSA key pair: G,R
ECDSA key pair generation	Generate a keypair for a requested elliptic curve	0	curve size	key pair	Random Number Generation Asymmetric Key Generation	Crypto Officer - DRBG seed, internal state V value, and key (IG D.L compliant): W,E - ECDSA key pair: G,R

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Safe primes key generation	Generate a keypair for a requested 'safe' domain parameter	0	key size	key pair	Random Number Generation Asymmetric Key Generation	Crypto Officer - DRBG seed, internal state V value, and key (IG D.L compliant): W,E - Diffie-Hellman key pair: G,R
Diffie-Hellman shared secret computation	Generate a shared secret	0	domain parameter, received public key and private key	shared secret	Shared Secret Computation	Crypto Officer - Diffie-Hellman key pair: W,E - Diffie-Hellman shared secret: G,R
EC Diffie-Hellman shared secret computation	Generate a shared secret	0	domain parameter, received public key and private key	shared secret	Asymmetric Key Validation Shared Secret Computation	Crypto Officer - EC Diffie Hellman key pair: W,E - EC Diffie-Hellman shared secret: G,R

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-test	execute pre operational self-tests and all conditional CASTs from section 10.2	N/A	power	pass/fail results	Symmetric Encryption and Decryption Key Wrapping Random Number Generation Message authentication (MAC) Asymmetric Key Generation Asymmetric Key Validation Digital Signature Generation Digital Signature Verification Shared Secret Computation Key Derivation (PBKDF) Key Derivation (KBKDF) Key Derivation (HKDF) Message Digest	Crypto Officer

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Return the module status	N/A	N/A	Status output	None	Crypto Officer
Show module and version info	Return Module Base Name and Module Version Number	N/A	N/A	Module information	None	Crypto Officer
Zeroization	SSPs are zeroised when the system is powered down, when all resources of symmetric crypto function context, all resources of hash context, all resources of Diffie-Hellman context for Diffie-Hellman and EC Diffie-Hellman, all resources	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 - ECDSA key pair: Z - RSA key pair: Z - Entropy input string: Z - DRBG seed, internal state V value, and key (IG D.L compliant): Z - PBKDF derived

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	of asymmetric crypto function context and all resources of key derivation function context are released					key: Z - PBKDF password: Z - KBKDF key derivation key: Z - KBKDF derived key: Z - Diffie-Hellman key pair: Z - EC Diffie Hellman key pair: Z - Diffie-Hellman shared secret: Z - EC Diffie-Hellman shared secret: Z
HKDF	Derive key from key derivation key from a shared secret	0	EC Diffie Hellman shared secret	HKDF derived key	Key Derivation (HKDF)	Crypto Officer - EC Diffie-Hellman shared secret: W,E - HKDF

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						derived key: G,R

Table 15: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
ANSI X9.63 KDF	Hash based Key Derivation Function	ANSI X9.63 KDF	CO
Blowfish	Encryption / Decryption	Blowfish	CO
CAST5	Encryption / Decryption Key Sizes: 40 to 128 bits in 8-bit increments	CAST5	CO
DES	Encryption / 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
EdDSA with Ed25519	Key Generation, Signature Generation, Signature Verification	EdDSA with Ed25519	CO
X25519 Key Agreement	Key agreement on X25519 curve	X25519 Key Agreement	CO
Integrated Encryption Scheme on elliptic curves	Encryption / Decryption	Integrated Encryption Scheme on elliptic curves	CO
MD2	Message Digest size: 128-bit	MD2	CO
MD4	Message Digest size: 128-bit	MD4	CO
RC2	Encryption / Decryption Key Sizes 8 to 1024-bits	RC2	CO
RC4	Encryption / 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	Key Pair Generation; keys < 2048-bits	RSA Keygen	CO

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Algorithms	Role
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]	Encrypt/Decrypt; 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
ML-KEM	Key Encapsulation Mechanism	ML-KEM	CO
Keccak	Message Digest	Keccak	CO

Table 16: Non-Approved Services

4.5 External Software/Firmware Loaded

The module does not support the loading of external software/firmware.

© 2025 Apple Inc., All rights reserved.

This document may be reproduced and distributed only in its original entirely 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-SHA256 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. It is automatically executed at power-on.

© 2025 Apple Inc., All rights reserved.

This document may be reproduced and distributed only in its original entirely 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 Device OS, a commercially available general-purpose operating system executing on the computing platforms specified in section 2.2.

© 2025 Apple Inc., All rights reserved.

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

7 Physical Security

The FIPS 140-3 physical security requirements do not apply to the Apple corecrypto Module 18.3 [Apple silicon, User, Software, SL1] since it is a software module.

© 2025 Apple Inc., All rights reserved.

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

8 Non-Invasive Security

Per IG 12.A, until the requirements of NIST SP 800-140F are defined, non-invasive mechanisms fall under ISO/IEC 19790:2012 Section 7.12 Mitigation of other attacks.

The requirements of this area are not applicable to the module.

© 2025 Apple Inc., All rights reserved.

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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 the 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

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

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Context object destruction	SSPs are zeroised when the appropriate context object is destroyed	Zeroization when structure is deallocated. The successful completion of the destruction routine indicates that the zeroization was successful.	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. The successful removal of power	Operator can initiate power down

© 2025 Apple Inc., All rights reserved.

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

Zeroization Method	Description	Rationale	Operator Initiation
		indicates that the zeroization was successful.	
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. The completion of the key generation routine indicates that the zeroization was successful	N/A

Table 19: SSP Zeroization Methods

Data output interfaces are inhibited while zeroisation is performed.

9.4 SSPs

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 - CSP			Symmetric Encryption and Decryption Message authentication (MAC)
AES key-wrapping key	AES KW	128 to 256 bits - 128 to 256 bits	symmetric - CSP			Key Wrapping
HMAC key	HMAC key	8 - 262144 bits - 112 to 256-bits	MAC - CSP			Message authentication (MAC)
ECDSA key pair	ECDSA key pair (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112 to 256 bits	Asymmetric - CSP	Asymmetric Key Generation		Digital Signature Generation Digital Signature Verification

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA key pair	RSA key pair (including intermediate keygen values)	2048 - 4096 bits - 112 to 150 bits	Asymmetric - CSP	Asymmetric Key Generation		Digital Signature Generation Digital Signature Verification
Entropy input string	Entropy input string	512 bits - 256 bits	Entropy input string - CSP			Random Number Generation
DRBG seed, internal state V value, and key (IG D.L compliant)	DRBG input parameters	384 bits - 256 bits	DRBG - CSP	Random Number Generation		Random Number Generation
PBKDF derived key	PBKDF derived key	128 to 256 bits - 128 to 256 bits	Storage key - CSP	Key Derivation (PBKDF)		
PBKDF password	PBKDF password	64 to 1024 bits - N/A	Password - CSP			Key Derivation (PBKDF)
KBKDF key derivation key	KBKDF key derivation key	128 to 256 bits - 128 to 256 bits	Derivation key - CSP			Key Derivation (KBKDF)
KBKDF derived key	KBKDF derived key	128 to 256 bits - 128 to 256 bits	Derived key - CSP	Key Derivation (KBKDF)		
Diffie-Hellman key pair	Diffie-Hellman key pair	MODP-2048, MODP-	Asymmetric - CSP	Asymmetric Key Generation		Shared Secret Computation

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(including intermediate keygen values)	3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits				
Diffie-Hellman shared secret	Diffie-Hellman shared secret	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits	Asymmetric - CSP		Shared Secret Computation	Key Derivation (HKDF)
EC Diffie Hellman key pair	EC Diffie-Hellman key pair (including intermediate keygen values)	P-224, P-256, P-384, P-521 - 112-256 bits	Asymmetric - CSP	Asymmetric Key Generation		Key Derivation (HKDF)
EC Diffie-Hellman shared secret	EC Diffie-Hellman shared secret	P-224, P-256, P-384, P-521 - 112-256 bits	Asymmetric - CSP		Shared Secret Computation	
HKDF derived key	HKDF key derived from EC Diffie-	2048 - 256	Derived key - CSP	Key Derivation (HKDF)		Key Derivation (HKDF)

© 2025 Apple Inc., All rights reserved.

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Hellman shared secret					

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	
ECDSA key pair	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	DRBG seed, internal state V value, and key (IG D.L compliant):Derived From
RSA key pair	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	DRBG seed, internal state V value, and key (IG D.L compliant):Derived From

© 2025 Apple Inc., All rights reserved.

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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Entropy input string		RAM:Plaintext	Storage duration during the usage of the CSP	Power down	DRBG seed, internal state V value, and key (IG D.L compliant):Generates
DRBG seed, internal state V value, and key (IG D.L compliant)		RAM:Plaintext	Storage duration during the usage of the CSP	Power down	Entropy input string:Derived From
PBKDF derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF password:Derived From
PBKDF password	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	PBKDF derived key:Derives
KBKDF key derivation key	API input parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KBKDF derived key:Derives
KBKDF derived key	API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	KBKDF key derivation key:Derived From
Diffie-Hellman key pair	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down Intermediate value zeroization	Diffie-Hellman shared secret:Generates

© 2025 Apple Inc., All rights reserved.

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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Diffie-Hellman shared secret	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	Diffie- Hellman key pair:Derived From
EC Diffie Hellman key pair	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 shared secret:Generates
EC Diffie-Hellman shared secret	API input parameters API output parameters	RAM:Plaintext	From service invocation to service completion	Context object destruction Power down	EC Diffie Hellman key pair:Derived From
HKDF derived key	API output parameters		From service invocation to service completion	Context object destruction Power down	EC Diffie-Hellman shared secret:Derived From

Table 21: SSP Table 2

9.5 Transitions

SHA-1 is disallowed for digital signature generation. When used for digital signature verification, SHA-1 is allowed for legacy use. The use of SHA-1 is deprecated through December 31, 2030, for applying protection in non-digital signature applications and disallowed thereafter. The use of SHA-1 is acceptable for processing already-protected information through December 31, 2030, and allowed for legacy use thereafter.

© 2025 Apple Inc., All rights reserved.

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

10 Self-Tests

While the module is executing the self-tests, services are not available, and input and output are inhibited.

10.1 Pre-Operational Self-Tests

The module performs a pre-operational software integrity automatically when the module is loaded into memory (i.e., at power on) before the module transitions to the operational state. A software integrity test is performed on the runtime image of the module with HMAC-SHA256 used to perform the approved integrity technique. Prior to using HMAC-SHA-256, a Conditional Cryptographic Algorithm Self-Tests (CAST) is performed.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A5986)	112-bit key	Message Authentication	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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM encrypt	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric encryption	Test runs at power-on before the integrity test
AES-GCM decrypt	128-bit key, decrypt	KAT	CAST	Module becomes operational	Symmetric decryption	Test runs at power-on before the integrity test
AES-CBC	128-bit key encrypt	KAT	CAST	Module becomes operational	Symmetric encryption	Test runs at power-on before first

© 2025 Apple Inc., All rights reserved.

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						use of the algorithm
AES-ECB	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric decryption	Test runs at power-on before first use of the algorithm
Counter DRBG	128-bit key	KAT	CAST	Module becomes operational	SP 800-90Ar1 (instantiate, reseed, generate) health test per section 11.3	Test runs at power-on before first use of the algorithm
HMAC-SHA2-256	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA3-224 (A6510)	SHA3-224	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3	P-224 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before first use of the algorithm

© 2025 Apple Inc., All rights reserved.

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-FFC-SSC Sp800-56Ar3	MODP-2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before first use of the algorithm
PBKDF	SHA-1, SHA-256, SHA-512	KAT	CAST	Module becomes operational	Password-based key derivation	Test runs at power-on before first use of the algorithm
Safe Primes Key Generation	MODP-2048	PCT	PCT	Successful key pair generation	SP 800-56A Rev. 3 Section 5.6.2.1.4	Key pair generation
ECDSA KeyGen (FIPS186-5)	P-224, P-256, P-384, P-521	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA SigGen (FIPS186-5)	P-224 curve with SHA-224	KAT	CAST	Module becomes operational	Signature generation & verification	Test runs at power-on before first use of the algorithm
ECDSA SigVer (FIPS186-5)	P-224 curve with SHA-224	KAT	CAST	Module becomes operational	Signature generation & verification	Test runs at power-on before first use of the algorithm
RSA KeyGen (FIPS186-5)	2048, 3072, 4096 - bit modulus	PCT	PCT	Module Successful key pair generation becomes operational	Signature generation & verification	Key pair generation
RSA SigGen (FIPS186-5)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Signature generation & verification	Test runs at power-on before first use of the algorithm

© 2025 Apple Inc., All rights reserved.

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-5)	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Signature generation & verification	Test runs at power-on before first use of the algorithm
KDA HKDF SP800-56Cr2	SHA-1, SHA2-256, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. with 256-bit secret	KAT	CAST	Module becomes operational	Shared secret key derivation	Test runs at power-on before first use of the algorithm
KDF SP800-108	SHA-1, SHA2-256, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. with 256-bit secret	KAT	CAST	Module becomes operational	key based key derivation	Test runs at power-on before first use of the algorithm

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5986)	Message Authentication	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 encrypt	KAT	CAST	On Demand	Manually

© 2025 Apple Inc., All rights reserved.

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

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM decrypt	KAT	CAST	On Demand	Manually
AES-CBC	KAT	CAST	On Demand	Manually
AES-ECB	KAT	CAST	On Demand	Manually
Counter DRBG	KAT	CAST	On Demand	Manually
HMAC-SHA2-256	KAT	CAST	On Demand	Manually
HMAC-SHA-1	KAT	CAST	On Demand	Manually
HMAC-SHA2-512	KAT	CAST	On Demand	Manually
HMAC-SHA3-224 (A6510)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3	KAT	CAST	On Demand	Manually
PBKDF	KAT	CAST	On Demand	Manually
Safe Primes Key Generation	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5)	PCT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-5)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-5)	PCT	PCT	On Demand	Manually
RSA SigGen (FIPS186-5)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5)	KAT	CAST	On Demand	Manually
KDA HKDF SP800-56Cr2	KAT	CAST	On Demand	Manually
KDF SP800-108	KAT	CAST	On Demand	Manually

Table 25: Conditional Periodic Information

© 2025 Apple Inc., All rights reserved.

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

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	1) The HMAC-SHA-256 value computed over the module did not match the pre-computed 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) Pre-operational Software Integrity Test failure or 2) Conditional CAST failure 3) Conditional PCT failure	Power cycle the device which results in the module being reloaded into memory and reperforming the pre-operational software integrity test and the Conditional CASTs.	1) Error message "FAILED: fipspost_post_integrity" sent 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

10.5 Operator Initiation of Self-Tests

The module permits operators to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module by rebooting the system (i.e., power-cycling).

© 2025 Apple Inc., All rights reserved.

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

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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

This digital signature-based integrity protection during the delivery/integration process is not to be confused with the HMAC-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 Table - Non-Approved Services. 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 requirements and restrictions in above section 2.7 when using the module.

© 2025 Apple Inc., All rights reserved.

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

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-1736.80.2 binary file listed in Table 2.

© 2025 Apple Inc., All rights reserved.

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

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.

© 2025 Apple Inc., All rights reserved.

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