Apple Inc.

Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1]
FIPS 140-3 Non-Proprietary Security Policy

September 2024

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

www.atsec.com

Trademarks

Apple's trademarks applicable to this document are listed in https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html.

Other company, product, and service names may be trademarks or service marks of others.

Table of Contents

List of Tables

1 General

This document is the non-proprietary FIPS 140-3 Security Policy for Apple corecrypto Module v12.0 [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.

This document provides all tables and diagrams (when applicable) required by NIST SP 800-140B. The column names of the tables follow the template tables provided in NIST SP 800-140B.

Table 1 describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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	Not Applicable
8	Non-invasive Security	Not Applicable
9	Sensitive Security Parameter Management	1
10	Self-tests	1
11	Life-cycle Assurance	1
12	Mitigation of Other Attacks	Not Applicable

Table 1 - Security Levels

2 Cryptographic Module Specification

The Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] cryptographic module (hereafter referred to as "the module") is a Software module running on a multi-chip standalone general-purpose computing platform. The version of module is 12.0. The module provides implementations of low-level cryptographic primitives to the Device OS's (iOS 15, iPadOS 15, watchOS 8, tvOS 15, T2OS 12 and macOS 12 Monterey) Security Framework and Common Crypto.

2.1 Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	iPadOS 15	iPad (5th generation)	Apple A Series A9	With and without PAA
2	iPadOS 15	iPad Pro 9.7-inch	Apple A Series A9X	With and without PAA
3	iPadOS 15	iPad (7th generation)	Apple A Series A10 Fusion	With and without PAA
4	iPadOS 15	iPad Pro 10.5-inch	Apple A Series A10X Fusion	With and without PAA
5	iPadOS 15	iPad mini (5th generation)	Apple A Series A12 Bionic	With and without PAA
6	iPadOS 15	iPad Pro 11-inch (1st generation)	Apple A Series A12X Bionic	With and without PAA
7	iPadOS 15	iPad Pro 11-inch (2nd generation)	Apple A Series A12Z Bionic	With and without PAA
8	iPadOS 15	iPad (9th generation)	Apple A Series A13 Bionic	With and without PAA
9	iPadOS 15	iPad Air (4th generation)	Apple A Series A14 Bionic	With and without PAA
10	iPadOS 15	iPad mini (6th generation)	Apple A Series A15 Bionic	With and without PAA
11	iPadOS 15	iPad Pro 11-inch (3rd generation)	Apple M Series M1	With and without PAA
12	iOS 15	iPhone 6S	Apple A Series A9	With and without PAA
13	iOS 15	iPhone 7 Plus	Apple A Series A10 Fusion	With and without PAA
14	iOS 15	iPhone X	Apple A Series A11 Bionic	With and without PAA
15	iOS 15	iPhone XS Max	Apple A Series A12 Bionic	With and without PAA
16	iOS 15	iPhone 11 Pro	Apple A Series A13 Bionic	With and without PAA
17	iOS 15	iPhone 12	Apple A Series A14 Bionic	With and without PAA
18	iOS 15	iPhone 13 Pro Max	Apple A Series A15 Bionic	With and without PAA
19	watchOS 8	Apple Watch Series S3	Apple S Series S3	With and without PAA
20	watchOS 8	Apple Watch Series S4	Apple S Series S4	With and without PAA

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
21	watchOS 8	Apple Watch Series S5	Apple S Series S5	With and without PAA
22	watchOS 8	Apple Watch Series S6	Apple S Series S6	With and without PAA
23	watch OS 8	Apple Watch Series S7	Apple S Series S7	With and without PAA
24	tvOS 15	Apple TV 4K	Apple A Series A10X Fusion	With and without PAA
25	tvOS 15	Apple TV 4K (2nd generation)	Apple A Series A12 Bionic	With and without PAA
26	T2OS 12	Apple Security Chip T2	Apple T Series T2	With and without PAA
27	macOS 12 Monterey	MacBook Pro (13-inch, M1, 2020)	Apple M Series M1	With and without PAA
28	macOS 12 Monterey	MacBook Pro 14-inch	Apple M Series M1 Pro	With and without PAA
29	macOS 12 Monterey	MacBook Pro 16-inch	Apple M Series M1 Max	With and without PAA

Table 2 - Tested Operational Environments

2.2 Vendor-affirmed Operational Environments

#	Operating System	Hardware Platform
1	iPadOS 15	iPad Pro 12.9-inch
2	iPadOS 15	iPad (6th generation)
3	iPadOS 15	iPad Pro 12.9-inch (2nd generation)
4	iPadOS 15	iPad Air (3rd generation)
5	iPadOS 15	iPad (8th generation)
6	iPadOS 15	iPad Pro 12.9-inch (3rd generation)
7	iPadOS 15	iPad Pro 12.9-inch (4th generation)
8	iPadOS 15	iPad Pro 12.9-inch (5th generation)
9	iOS 15	iPhone SE
10	iOS 15	iPhone 6S Plus
11	iOS 15	iPhone 7
12	iOS 15	iPhone 8
13	iOS 15	iPhone 8 Plus
14	iOS 15	iPhone XS
15	iOS 15	iPhone XR
16	iOS 15	iPhone 11
17	iOS 15	iPhone 11 Pro Max
18	iOS 15	iPhone SE (2nd generation)
19	iOS 15	iPhone 12 mini

20	iOS 15	iPhone 12 Pro
21	iOS 15	iPhone 12 Pro Max
22	iOS 15	iPhone 13 mini
23	iOS 15	iPhone 13
24	iOS 15	iPhone 13 Pro
25	watchOS 8	Apple Watch SE
26	macOS 12 Monterey	MacBook Air
27	macOS 12 Monterey	Mac mini
28	macOS 12 Monterey	iMac (24-inch)

Table 3 - Vendor Affirmed Operational Environments

The 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 Modes of operation

The module operates in Approved and Non-Approved mode of operation. The mode is implicit and is based on the service utilized.

The module is in the Approved mode of operation when the module utilizes the services that use the security functions listed in the Table 5 ,Table 6 and Table 7. 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 14 - Non-Approved Services. If the device starts up successfully, then the module has passed all self-tests and is operating in the Approved 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 Table 5,Table 6 and Table 7	Approved	return a '1' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was approved
Non-Approved mode	Non-Approved mode of operation is entered when the module utilizes non-approved security functions in Table 8.	Non-Approved	return a '0' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was non-approved

Table 4 - Modes of Operation

2.4 Vendor Affirmed Algorithms

Algorithm	Caveat	Use / Function
CKG [SP800-133rev2] (asymmetric)	vendor affirmed	Cryptographic key Generation for asymmetric (RSA/EC and DH) key pair; FIPS 140-3 IG D.H and SP800-133rev2 section 4 example 1

Table 5 - Vendor Affirmed Approved Algorithms

2.5 Approved Algorithms

The table below lists all Approved security functions of the module, including specific key size(s) -in bits otherwise noted- employed for approved services. Not all algorithms tested with CAVP are used by the module.

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2783, A2802 (asm_arm)	AES [FIPS 197; SP 800-38A]	CBC	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	CBC	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2785, A2804 (c_glad)	AES [FIPS 197; SP 800-38A]	CBC	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	CBC	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2787, A2806 (vng_asm)	AES [FIPS 197; SP 800-38C]	CCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38C]	CCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38C]	CCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2783, A2802 (asm_arm)	AES [FIPS 197; SP 800-38A]	CFB128	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	CFB128	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	CFB128	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	CFB8	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	CFB8	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38B]	CMAC	Key Size / Key Strength: 128, 192, 256 bits	Message authentication (MAC)
A2787, A2806 (vng_asm)	AES [FIPS 197; SP 800-38A]	CTR	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	CTR	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	CTR	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2783, A2802 (asm_arm)	AES [FIPS 197; SP 800-38A]	ECB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2787, A2806 (vng_asm)	AES [FIPS 197; SP 800-38A]	ECB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	ECB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	ECB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2787, A2806 (vng_asm)	AES [FIPS 197; SP 800-38D]	GCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38D]	GCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38D]	GCM	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2783, A2802 (asm_arm)	AES [FIPS 197; SP 800-38A]	OFB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38A]	OFB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38A]	OFB	Key Size / Key Strength: 128, 192, 256 bits	Symmetric Encryption and Decryption
A2783, A2802 (asm_arm)	AES [FIPS 197; SP 800-38E]	XTS	Key Size / Key Strength: 128, 256 bits	Symmetric Encryption and Decryption
A2786, A2805 (c_ltc)	AES [FIPS 197; SP 800-38E]	XTS	Key Size / Key Strength: 128, 256 bits	Symmetric Encryption and Decryption
A2784, A2803 (c_asm)	AES [FIPS 197; SP 800-38E]	XTS	Key Size / Key Strength: 128, 256 bits	Symmetric Encryption and Decryption
A2787, A2806 (vng_asm)	DRBG [SP800-90Arev1]	CTR_DRBG: AES-128, AES-256	Key Size / Key Strength: 128, 256 bits Derivation Function Enabled, No Prediction Resistance	Random Number Generation
A2786, A2805 (c_ltc)	DRBG [SP800-90Arev1]	CTR_DRBG: AES-128, AES-256	Key Size / Key Strength: 128, 256 bits Derivation Function Enabled, No Prediction Resistance	Random Number Generation
A2784, A2803 (c_asm)	DRBG [SP800-90Arev1]	CTR_DRBG: AES-128, AES-256	Key Size / Key Strength: 128, 256 bits Derivation Function Enabled, No Prediction Resistance	Random Number Generation
A2788, A2807 (vng_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	Key Pair Generation (CKG using method in Section 4 [SP 800-133Rev2]) [FIPS 186-4] Appendix B.4.2 Testing Candidates	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Asymmetric Key Generation
A2786, A2805 (c_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	Key Pair Generation (CKG using method in Section 4 [SP 800-133Rev2]) [FIPS 186-4] Appendix B.4.2 Testing Candidates	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Asymmetric Key Generation

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2788, A2807 (vng_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	N/A	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Key Validation
A2786, A2805 (c_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	N/A	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Key Validation
A2788, A2807 (vng_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	SHA2-224, SHA2-256, SHA2-384, SHA2-512	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Digital Signature Generation
A2786, A2805 (c_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	SHA2-224, SHA2-256, SHA2-384, SHA2-512	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Digital Signature Generation
A2788, A2807 (vng_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	SHA-1 (legacy), SHA2-224, SHA2-256, SHA2-384, SHA2-512	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Digital Signature Verification
A2786, A2805 (c_ltc)	ECDSA ANSI X9.62 [FIPS 186-4]	SHA-1(legacy), SHA2-224, SHA2-256, SHA2-384, SHA2-512	: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Digital Signature Verification
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-1	Key Size: 128 - 262144 bits Key Strength: 128 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-1	Key Size: 128 - 262144 bits Key Strength: 128 bits	Message authentication (MAC)
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-224	Key Size: 224 - 262144 bits Key Strength: 224 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-224	Key Size: 224 - 262144 bits Key Strength: 224 bits	Message authentication (MAC)
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-256	Key Size: 224 - 262144 bits Key Strength: 256 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-256	Key Size: 256 - 262144 bits Key Strength: 256 bits	Message authentication (MAC)
A2789, A2808 (vng_neon)	HMAC [FIPS 198]	SHA-256 (for all CPUs in Table 2 except S3)	Key Size: 256 - 262144 bits Key Strength: 256 bits	Message authentication (MAC)
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-384	Key Size: 384 - 262144 bits Key Strength: 384 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-384	Key Size: 384 - 262144 bits Key Strength: 384 bits	Message authentication (MAC)
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-512	Key Size: 512 - 262144 bits Key Strength: 512 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-512	Key Size: 512 - 262144 bits Key Strength: 512 bits	Message authentication (MAC)
A2788, A2807 (vng_ltc)	HMAC [FIPS 198]	SHA-512/256	Key Size: 512 - 262144 bits Key Strength: 256 bits	Message authentication (MAC)

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2786, A2805 (c_ltc)	HMAC [FIPS 198]	SHA-512/256	Key Size: 512 - 262144 bits Key Strength: 256 bits	Message authentication (MAC)
A2786, A2805 (c_ltc)	KAS-ECC-SSC [SP800-56Arev 3]	Scheme: ephemeral Unified KAS Role: initiator, responder	Curve: P-224, P-256, P-384, P-521 Key Strength: from 112 - 256 bits	Shared Secret Computation
A2786, A2805 (c_ltc)	KAS-FFC-SSC [SP800-56Arev3]	Scheme: dh Ephem with safe prime groups KAS Role: initiator, responder	Key Size: MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192. Key Strength: from 112 - 200 bits	Shared Secret Computation
A2788, A2807 (vng_ltc) A2786, A2805 (c_ltc)	KBKDF [SP800-108rev1]	KDF Mode: Counter and Feedback MAC Mode: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Key Size / Key Strength: 128 -256 bits Supported [output] Lengths: 8-4096 Increment 8 Fixed Data Order: Before Fixed Data Counter Length: 32	Key Derivation
A2786, A2805 (c_ltc)	KBKDF [SP800-108rev1]	KDF Mode: Counter MAC Mode: CMAC-AES128, CMAC-AES192, CMAC-AES256	Key Size / Key Strength: 128 - 256 bits Supported [output] Lengths: 8-4096 Increment 8 Fixed Data Order: Before Fixed Data Counter Length: 8, 16, 24, 32	Key Derivation
A2786, A2805 (c_ltc)	KTS (AES) [FIPS 197; SP 800-38 F]	AES-KW	Key Size / Key Strength: 128, 192, 256 bits	Key Wrapping
A2784, A2803 (c_asm)	KTS (AES) [FIPS 197; SP 800-38 F]	AES-KW	Key Size / Key Strength: 128, 192, 256 bits	Key Wrapping
A2788, A2807 (vng_ltc)	PBKDF [SP800-132]	HMAC with: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Key Size / Key Strength: 128 - 256 bits Password length: 8- 128 bytes Increment 1 Salt Length: 128-4096 Increment 8 Iteration Count: 10-1000 Increment 1	Key Derivation
A2786, A2805 (c_ltc)	PBKDF [SP800-132]	HMAC with: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Key Size / Key Strength: 128 - 256 bits Password length: 8- 128 bytes Increment 1 Salt Length: 128-4096 Increment 8 Iteration Count: 10-1000 Increment 1	Key Derivation
A2788, A2807 (vng_ltc)	RSA [FIPS 186-4]	ANSI X9.31; CKG using method in Section 4 example 1 [SP 800-133Rev2]	Key Size: 2048, 3072, 4096 bits Key Strength: from 112 - 150 bits	Asymmetric Key Generation
A2786, A2805 (c_ltc)	RSA [FIPS 186-4]	ANSI X9.31; CKG using method in Section 4 example 1 [SP 800-133Rev2]	Key Size: 2048, 3072, 4096 bits Key Strength: from 112 - 150 bits	Asymmetric Key Generation
A2788, A2807 (vng_ltc)	RSA [FIPS 186-4]	PKCS#1 v1.5: and PKCS PSS	Key Size: 2048, 3072, 4096 bits Key Strength: from 112 - 150 bits	Digital Signature Generation
A2786, A2805 (c_ltc)	RSA [FIPS 186-4]	PKCS#1 v1.5 and PKCS PSS	Key Size: 2048, 3072, 4096 bits Key Strength: from 112 - 150 bits	Digital Signature Generation

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2788, A2807 (vng_ltc)	RSA [FIPS 186-4]	PKCS#1 v1.5 and PKCS PSS	Key Size: 1024 (legacy), 2048, 3072, 4096 bits Key Strength: from 80 - 150 bits	Digital Signature Verification
A2786, A2805 (c_ltc)	RSA [FIPS 186-4]	PKCS#1 v1.5 and PKCS PSS	Key Size: 1024 (legacy), 2048, 3072, 4096 bits Key Strength: from 80 - 150 bits	Digital Signature Verification
A2786, A2805 (c_ltc)	Safe Primes Key Generation	CKG using method in Section 4 example 1 [SP 800-133Rev2)	Safe Prime Groups: MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192; Key Strength: from 112 - 200 bits	Key Generation
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-1	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-1	N/A	Message Digest
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-224	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-224	N/A	Message Digest
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-256	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-256	N/A	Message Digest
A2789, A2808 (vng_neon)	SHS [FIPS 180-4]	SHA-256 (for all CPUs in Table 2 except S3)	N/A	Message Digest
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-384	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-384	N/A	Message Digest
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-512	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-512	N/A	Message Digest
A2788, A2807 (vng_ltc)	SHS [FIPS 180-4]	SHA-512/256	N/A	Message Digest
A2786, A2805 (c_ltc)	SHS [FIPS 180-4]	SHA-512/256	N/A	Message Digest

Table 6 - Approved Algorithms

2.6 Non-Approved Algorithms Allowed in the Approved Mode of Operation

There are no non-Approved but “Allowed functions” with security claimed algorithms in approved mode.

2.7 Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use/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 7 - Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

2.8 Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Algorithm/Functions	Use / Function
RSA Key Pair Generation	ANSI X9.31 Key Pair Generation Key Size < 2048
RSA Signature Generation	PKCS#1 v1.5 and PSS Signature Generation Key Size < 2048
RSA Signature Verification	PKCS#1 v1.5 and PSS Signature Verification Key Size < 1024
RSA Key Wrapping	OAEP, PKCS#1 v1.5 and PSS schemes
Diffie-Hellman	Shared Secret Computation using key size < 2048
EC Diffie-Hellman	Shared Secret Computation using curves < P-224
EdDSA	Key Generation with Ed25519 Signature Generation with Ed25519 Signature Verification with Ed25519 Key Agreement with X25519
ANSI X9.63 KDF	Hash based Key Derivation Function
RFC6637	Key Derivation Function
HKDF [SP800-56Crev2]	Key Derivation Function
DES	Encryption / Decryption Key Size 56-bits
CAST5	Encryption / Decryption Key Sizes 40 to 128-bits in 8-bit increments
AES-GCM using external IV	Authenticated Encryption / Decryption
RC4	Encryption / Decryption Key Sizes 8 to 4096-bits
RC2	Encryption / Decryption Key Sizes 8 to 1024-bits
MD2	Message Digest Digest size 128-bit
MD4	Message Digest Digest size 128-bit
RIPEMD	Message Digest Digest size 160-bits
ECDSA	PKG: Curve P-192 with security strength of 96 bits PKV: Curve P-192 Signature Generation: Curve P-192 Signature Verification: Curve P-192
ECDSA	Key Pair Generation for compact point representation of points

Algorithm/Functions	Use / Function
Integrated Encryption Scheme on elliptic curves (ECIES)	Hybrid Encryption scheme
Blowfish	Encryption / Decryption
OMAC (One-Key CBC MAC)	MAC generation / verification
Triple-DES [SP 800-67]	Encryption/Decryption with modes CBC, CTR, CFB64, ECB, CFB8, OFB

Table 8 - Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.9 Module components

Package/File Names	Software Version	Integrity Test Implemented
corecrypto-1217.40.11	12.0	HMAC-SHA-256

Table 9 - Executable Code Sets

The module cryptographic boundary is delineated by the dotted green rectangle in the Figure 1. The Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] executes within the user space of the computing platforms and operating systems listed in Table 2.

The tested operational environment's physical perimeter (TOEPP) is represented by the most exterior black line in the block diagram Figure 1.

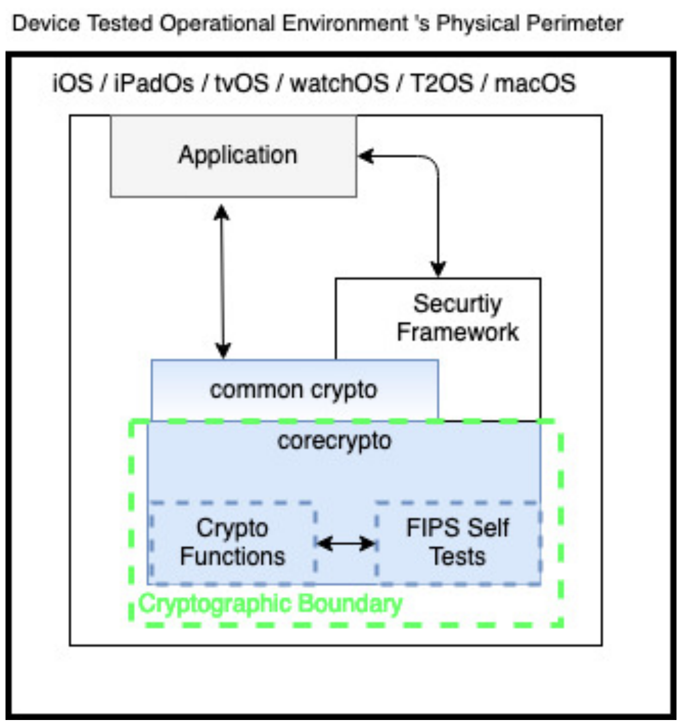

Figure 1 - Block diagram

3 Cryptographic Module Interfaces

The underlying logical interfaces of the module are the C language Application Programming Interfaces (APIs). In detail these interfaces are described in (Table 10):

Physical Ports	Logical Interface[1]	Data that passes over port/interface
As a software-only module, the module does not have physical ports. Physical Ports are interpreted to be the physical ports of the hardware platform on which it runs	Data Input	Data inputs are provided in the variables passed in the API and callable service invocations, generally through caller-supplied buffers
	Data Output	Data outputs are provided in the variables passed in the API and callable service invocations, generally through caller-supplied buffers
	Control Input	Control inputs which control the mode of the module are provided through dedicated parameters.
	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 10 - Ports and Interfaces

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 dynamically loadable 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.

[1] The module does not implement a Control Output Logical Interface

4 Roles, services, and authentication

4.1 Roles

The module supports a single instance of one authorized role: the Crypto Officer. No support is provided for multiple concurrent operators.

Name	Type	Operator Type	Authentication Method
Crypto Officer	Role	CO	Implicit

Table 11 - Roles

4.2 Authentication

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 - Approved Services and - Non-Approved Services below).

4.3 Services

Name	Type	Description	SF Properties	Algorithm / CAVP Cert
KAS-ECC	KAS	EC Diffie-Hellman Shared Secret computation SP 800-56ARev3. KAS-ECC per IG D.F Scenario 2 path (1)	Curves P-224, P-256, P-384, P-521 providing from 112 to 256 bits of encryption strength	KAS-ECC-SSC SP800-56ARev3 / A2786, A2805
KAS-FFC	KAS	Diffie-Hellman Shared Secret Computation KAS-FFC per IG D.F Scenario 2 path (1).	Safe Prime Groups MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 providing from 112 to 200 bits of encryption strength	KAS-FFC-SSC SP800-56ARev3/ A2786, A2805
KTS	KTS	SP 800-38F, IG D.G. AES key wrapping and unwrapping	128, 192, and 256-bit AES keys providing 128, 192, or 256 bits of encryption strength	AES-KW/ A2786, A2805 AES-KW/ A2784, A2803

Table 12 - Security Function Implementations

The module implements a dedicated API function (section "Modes of Operation" above) to indicate if a requested service utilizes an approved security function. For services listed in Table Approved Services, the indicator function returns 1.

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
Symmetric Encryption	Execute AES-mode encrypt operation	1	AES key, plaintext data	ciphertext data	AES-CBC, AES-ECB, AES-CFB128, AES-CFB8, AES-OFB, AES-CTR, AES-XTS, AES-GCM, AES-CCM	CO	W,E
Symmetric Decryption	Execute AES-mode decrypt operation	1	AES key, ciphertext data	plaintext data	AES-CBC, AES-ECB, AES-CFB128, AES-CFB8, AES-OFB, AES-CTR, AES-XTS, AES-GCM, AES-CCM	CO	W,E

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
Key Wrapping	Execute AES-key wrapping operation	1	AES key-wrapping key, unwrapped key	wrapped key	AES-KW	CO	W, E
Key Unwrapping	Execute AES-key unwrapping operation	1	AES key- wrapping key, wrapped key	unwrapped key	AES-KW	CO	W, E
Message Digest Generation	Generate a digest for the requested algorithm	1	Message	message digest	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256, MD5[2]	CO	N/A
Message Authentication Code (CMAC/HMAC) Generation	Generate a Message Authentication Code	1	HMAC key or AES key, MAC algorithm, message	MAC	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/256, AES-CMAC	CO	W, E
Message Authentication Code (CMAC) Verification	Verify a Message Authentication Code	1	MAC, message, AES key	pass/fail	AES-CMAC	CO	W, E
Signature generation (RSA)	Sign a message with a specified RSA private key.	1	RSA private key, message, hash algorithm	computed signature	RSA SigGen	CO	W, E
Signature verification (RSA)	Verify the signature of a message with a specified RSA public key.	1	RSA public key, digital signature, message, hash algorithm	pass/fail result of digital signature verification	RSA SigVer	CO	W, E
Signature generation (ECDSA)	Sign a message with a specified ECDSA private key	1	ECDSA private key, message, hash algorithm	computed signature	ECDSA SigGen	CO	W, E
Signature verification (ECDSA)	Verify the signature of a message with a specified ECDSA public key	1	ECDSA public key, digital signature, message, hash algorithm	pass/fail result of digital signature verification	ECDSA SigVer	CO	W, E
Random number generation	Generate Random number	1	Entropy Input, DRBG seed, Internal, state V value, and key	random bit-string	CTR_DRBG	CO	E/ G, W, E / G, W, E
Key Derivation (PBKDF)	Derive key from password	1	PBKDF password	PBKDF derived key	PBKDF	CO	W, E / G, R
Key Derivation (KBKDF)	Derive key from key derivation key	1	KBKDF key derivation key	KBKDF derived key	KBKDF	CO	W, E / G, R
Key pair generation (RSA)	Generate a keypair for a requested modulus	1	key size	RSA Key Pair	RSA KeyGen, CKG	CO	G, R
Key pair generation (ECDSA)	Generate a keypair for a requested elliptic curve	1	key size	ECDSA Key Pair	ECDSA KeyGen, CKG	CO	G, R
Public key validation (ECDSA)	Verify a public key for a requested elliptic curve	1	ECDSA public key	pass/fail result of key pair verification	ECDSA KeyVer	CO	E, W

[2] non-approved but allowed for TLS 1.0/1.1. Used in the context of TLS in conjunction with the approved algorithm SHA-1. No security claimed.

Name	Description	Indicator	Inputs	Outputs	Security Function Implementations	Roles	Roles SSP Access
Safe primes key generation	Generate a keypair for a requested 'safe' domain parameter	1	domain parameter	DH Key Pair	Safe primes key generation	CO	G, R
Diffie-Hellman Shared Secret Computation	Generate a shared secret	1	received DH public key, DH private key	DH shared secret	KAS-FFC-SSC	CO	W, E/ W, E/ G, R
EC Diffie-Hellman Shared Secret Computation	Generate a shared secret	1	received ECDH public key, ECDH private key	ECDH shared secret	KAS-ECC-SSC	CO	W, E/ W, E/ G, R
Zeroization	Release all resources of symmetric crypto function context	1	AES key	N/A	N/A	CO	Z
	Release all resources of hash context	1	HMAC key	N/A	N/A	CO	Z
	Release of all resources of Diffie-Hellman context for Diffie-Hellman and EC Diffie-Hellman	1	Asymmetric keys (ECDH/DH) and shared secret	N/A	N/A	CO	Z
	Release of all resources of asymmetric crypto function context	1	RSA/ ECDSA key pair	N/A	N/A	CO	Z
	Release of all resources of key derivation function context	1	KBKDF key derivation key, PBKDF password, KBKDF and PBKDF derived key	N/A	N/A	CO	Z
Self-test	Execute the CASTs	1	None	pass/fail results of self-tests	Algorithms listed in table Table 19	CO	N/A
Show Status	Return the module status	None	None	status output	N/A	CO	N/A
Show Module Info	Return Module Base Name and Module Version Number	None	None	name and version information	N/A	CO	N/A

Table 13 - Approved Services

The abbreviations of the access rights to 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.

N/A = The service does not access any SSP during its operation.

Name	Description	Algorithms Accessed	Role
Triple-DES encryption / decryption	Modes CBC, CTR, CFB64, ECB, CFB8, OFB	Triple-DES	CO
RSA Key Encapsulation	The CAST does not perform the full KTS, only the raw RSA encrypt/ decrypt.	RSA encrypt/ decrypt	CO

Name	Description	Algorithms Accessed	Role
RSA Key-pair Generation	ANSI X9.31 Key-pair Generation Key Size < 2048	RSA KeyGen	CO
RSA Signature Generation	PKCS#1 v1.5 and PSS Signature Generation Key Size < 2048	RSA Signature Generation	CO
RSA Signature Verification	PKCS#1 v1.5 and PSS Signature Verification Key Size < 1024	RSA Signature Verification	CO
Diffie Hellman Shared Secret Computation	for key sizes < 2048	Diffie Hellman Shared Secret Computation	CO
EC Diffie Hellman Shared Secret Computation	for curve sizes < P-224	EC Diffie Hellman Shared Secret Computation	CO
ECDSA Key-pair Generation (PKG) and ECDSA Key Validation (PKV)	ECDSA PKG and PKV using curve P-192	ECDSA Key Generation, ECDSA Key Validation	CO
ECDSA Signature Generation	ECDSA Signature Generation using curve P-192	ECDSA Signature Generation	CO
ECDSA Signature Verification	ECDSA Signature Verification using curve P-192	ECDSA Signature Verification	CO
ECDSA Key Pair Generation for compact point representation of points	Key Pair Generation for compact point representation of points	ECDSA Key Generation	CO
EdDSA Key Generation	Key Generation with Ed25519	EdDSA Key Generation	CO
EdDSA Signature Generation	Signature Generation with Ed25519	EdDSA Signature Generation	CO
EdDSA Signature Verification	Signature Verification with Ed25519	EdDSA Signature Verification	CO
EdDSA Key Agreement	Key Agreement with X25519	EdDSA Key Agreement	CO
ECIES	Elliptic Curve encrypt	ECIES Encrypt	CO
ANSI X9.63 Key Derivation	SHA-1 hash-based	SHA-1	CO
SP800-56Crev2 Key Derivation (HKDF)	SHA-256 hash-based	SHA-256	CO
RFC6637 Key Derivation	SHA hash based	SHA-256, SHA-512, AES-128, AES-256	CO
OMAC Message Authentication Code Generation and Verification	One-Key CBC-MAC using 128-bit key	OMAC	CO
Message digest generation	Message digest generation using non-approved algorithms	MD2, MD4 RIPEMD	CO
Authenticated Encryption / decryption	Encrypt a plaintext / Decrypt a ciphertext	AES-GCM using external IV	CO
(other) symmetric encryption / decryption	symmetric encryption / decryption using non-approved algorithms	Blowfish, CAST5, DES, RC2, RC4	CO

Table 14 - Non-Approved Services

5 Software/Firmware security

5.1 Integrity Techniques

The Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] which is made up of a single component, is provided in the form of binary executable code. 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 On-Demand Integrity Test

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, automatically executed at power-on.

6 Operational Environment

The Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] operates in a modifiable operational environment per FIPS 140-3 level 1 specifications. 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.

7 Physical Security

The FIPS 140-3 physical security requirements do not apply to the Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] since it is a software module.

8 Non-invasive Security

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

9 Sensitive Security Parameter Management

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

Key /SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and related keys
AES Key / CSP	128 - 256 bits	AES-CBC (A2783, A2784, A2785, A2786, A2802, A2803, A2804, A2805) AES-CCM (A2784, A2786, A2787, A2803, A2805, A2806) AES-CFB8, (A2784, A2786, A2803, A2805) AES-CFB128 (A2783, A2784, A2786, A2802, A2803, A2805) AES-CMAC (A2786, A2805) AES-CTR (A2784, A2786, A2787, A2803, A2805, A2806) AES-ECB (A2783, A2784, A2786. A2787, A2802, A2803, A2805, A2806) AES-GCM (A2784, A2786, A2787, A2803, A2805, A2806) AES- OFB (A2783, A2784, A2786, A2802, A2805, A2803) AES-XTS (A2783, A2784, A2786, A2802, A2803, A2805)	N/A	Import from calling application No Export	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: Symmetric Encryption and Decryption; message authentication code (CMAC) **Related keys**: N/A
AES key-wrapping Key / CSP	128 - 256 bits	AES-KW (A2784, A2803, A2786, A2805)	N/A	Import from calling application No Export	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: Key Wrapping **Related keys**: N/A
HMAC Key / CSP	128-256 bits	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/256 (A2788, A2807, A2786, A2805, A2789, A2808)	N/A	Import from calling application No Export	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: Message authentication code generation (HMAC) **Related keys**: N/A

Key /SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and related keys
ECDSA public key (including intermediate keygen values) / PSP	112 - 256 bits	ECDSA KeyGen (A2788, A2807, A2786, A2805)	The key pairs are generated conformant to SP800-133rev2 (CKG) using FIPS186-4 Key Generation method, and the random value used in the key generation is generated using SP800-90Arev1 DRBG	Import and Export to calling application for key pair only. Intermediate keygen values are not output.	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down. Intermediate keygen values are zeroized before the module returns from the key generation function.	**Use**: Digital Signature verification **Related keys**: DRBG internal state, ECDSA private key
ECDSA private key (including intermediate keygen values) / CSP								**Use**: Digital Signature generation **Related keys**: DRBG internal state, ECDSA public key
RSA public key (including intermediate keygen values) / PSP	112 - 150 bits	RSA KeyGen (A2788, A2807, A2786, A2805)	The key pairs are generated conformant to SP800-133rev2 (CKG) using FIPS186-4 Key Generation method, and the random value used in the key generation is generated using SP800-90Arev1 DRBG	Import and Export to calling application for key pair only. Intermediate keygen values are not output.	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down. Intermediate keygen values are zeroized before the module returns from the key generation function.	**Use**: Digital Signature verification **Related keys**: DRBG internal state, RSA private key
RSA private key (including intermediate keygen values) / CSP					N/A			**Use**: Digital Signature generation **Related keys**: DRBG internal state, RSA public key
DRBG Entropy Input / CSP (IG D.L)	256 bits	Random Number Generation E14, E15 (see PUD referenced in section 11.2)	Obtained from two entropy sources	N/A	N/A	RAM	When the system is powered down	**Use** Random Number Generation **Related keys**: DRBG seed
DRBG Seed / CSP (IG D.L)	256 bits	CTR_DRBG (A2787, A2806, A2786, A2805, A2784, A2803)	Derived from entropy input as defined by SP800-90Arev1	N/A	N/A	RAM	When the system is powered down	**Use**: Random Number Generation **Related keys**: DRBG entropy input, DRBG internal state

Key /SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and related keys
DRBG Internal State V value, and Key / CSP (IG D.L)	256 bits	CTR_DRBG (A2787, A2806, A2786, A2805, A2784, A2803)	Derived from seed as defined by SP800-90Arev1	N/A	N/A	RAM	When the system is powered down	**Use**: Random Number Generation **Related keys**: DRBG seed
PBKDF Derived Keys / CSP	128 - 256 bits	PBKDF (A2788 , A2807, A2786, A2805)	Internally generated via SP800-132 PBKDF	No Import Export to calling application	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: PBKDF Key Derivation **Related keys**: PBKDF password
PBKDF Password / CSP	N/A	PBKDF (A2788 , A2807, A2786, A2805)	N/A	imported from calling application No Export	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: PBKDF Key Derivation **Related keys**: PBKDF derived key
KBKDF Key Derivation Key / CSP	128 - 256 bits	KBKDF (A2788 , A2807, A2786, A2805)	N/A	imported from calling application No Export	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: KBKDF Key Derivation **Related keys**: KBKDF derived key
KBKDF Derived Key / CSP	128 - 256 bits	KBKDF (A2788 , A2807, A2786, A2805)	Generated via SP800-108rev1 KBKDF	No Import Export to calling application	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: KBKDF Key Derivation **Related keys**: KBKDF Key Derivation Key
DH public, private keys (including intermediate keygen values) / PSP-CSP	112 - 200 bits	KAS-FFC-SSC (A2786, A2805)	The key pairs are generated conformant to SP800-133rev2 (CKG) using Safe-prime groups MODP groups belonging to (RFC 3526)	Import from calling application Export to calling application	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down. Intermediate keygen values are zeroized before the	**Use**: Diffie-Hellman shared secret computation **Related keys**: DRBG internal state, Diffie-Hellman Shared Secret

Key /SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and related keys
							module returns from the key generation function.	
DH Shared Secret / CSP	112 - 200 bits	KAS-FFC-SSC (A2786, A2805)	N/A	No Import Export to calling application	Established using SP800-56Arev3 KAS-FFC-SSC	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: None **Related keys**:, DH private and public keys
ECDH public, private keys (including intermediate keygen values) / PSP-CSP	112 - 256 bits	KAS-ECC-SSC (A2786, A2805)	The key pairs are generated conformant to SP800-133rev2 (CKG) using FIPS 186-4 Key Generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import from and Export to calling application for key pair only. Intermediate keygen values are not output.	N/A	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down. Intermediate keygen values are zeroized before the module returns from the key generation function.	**Use**: ECDH Shared secret computation **Related keys**: EC Diffie-Hellman Shared Secret
ECDH Shared Secret	112 - 256 bits	KAS-ECC-SSC (A2786, A2805)	N/A	No Import Export to calling application	Established using SP800-56Arev3 KAS-ECC-SSC	RAM	Automatic zeroisation when structure is deallocated or when the system is powered down	**Use**: None **Related keys**: ECDH private and public keys

Table 15 - SSPs

9.1 Random Number Generation

The NIST SP 800-90Arev1 approved deterministic random bit generator is a CTR_DRBG based on block cipher. The CTR_DRBG is using AES-256 with derivation function and without prediction resistance. The module performs DRBG health tests according to section 11.3 of [SP800-90Arev1]. The deterministic random bit generators are seeded by /dev/random. The /dev/random is the User Space interface.

No non-DRBG functions or instances are able to access the DRBG internal state

Two entropy sources (one non-physical entropy source and one physical entropy source) residing within the TOEPP provide the random bits. The operator does not have the ability to modify the F5 entropy source (ES) configuration settings (see details in Public Use Document referenced in section 11.2).

The output of entropy pool provides 256-bits of entropy to seed and reseed SP800-90Arev1 DRBG during initialization (seed) and reseeding (reseed).

Entropy Sources	Minimum number of bits of entropy	Details
ESV #E14 (Apple corecrypto physical entropy source)	256 bits	The entropy source consists of twenty-four Free Ring Oscillator (FROs) with a vetted conditioning function SHA-256 (ACVP cert. # C1223)
ESV #E15 (Apple corecrypto non-physical entropy source)	256 bits	The non-physical entropy source is based upon interrupt timings with a vetted conditioning function SHA-256 (ACVP certs. # A2797, A2869)

Table 16 – Non-Deterministic Random Number Generation Specification

9.2 Key / SSP 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 (RSA/ EC and DH) per [SP800-133r2] section 4 example 1 (vendor affirmed), compliant with [FIPS186-4], and using DRBG compliant with [SP800-90A]. A seed (i.e., the random value) used in asymmetric key generation is obtained from [SP800-90A] DRBG. The key generation service for RSA, ECDSA, Diffie-Hellman and EC Diffie-Hellman as well as the [SP 800-90A] DRBG have been ACVT tested with algorithm certificates found in Table 6.
The key derivation functions are as follows:

- PBKDF Key Derivation

  The module implements a CAVP compliance tested key derivation function compliant to [SP800-132], 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 the option 1a specified in section 5.4 of [SP800-132]. The keys derived from [SP800-132] maps to section 4.1 of [SP800-133rev2] as indirect generation from DRBG. The derived keys may only be used in storage applications.

- KBKDF Key Derivation

  The KBKDF is compliant to [SP800-108rev1] and IG D.M. The module implements both Counter and Feedback modes with HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 as the Pseudorandom Function (PRF). The module implements Counter mode with CMAC-AES128, CMAC-AES192, CMAC-AES256 as the PRFs.

9.3 Keys/ SSPs Establishment

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

- AES-Key Wrapping

The module implements a Key Transport Scheme (KTS) using AES-KW compliant to [SP800-38F], IG D.G. The SSP establishment methodology provides between 128 and 256 bits of encryption strength.

- Diffie-Hellman Shared Secret Computation

  The module provides SP800-56Arev3 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 SP800-56Arev3 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.

9.4 Keys/SSPs Import/Export

All keys and SSPs that are entered from, or output to module, are entered from or output to the invoking application running on the same device. Keys/SSPs entered into the module are electronically entered in plain text form. The module only outputs asymmetric keys in plain text form when key generation service is requested by the calling application.

9.5 Keys/SSPs Storage

Name	Description	Persistence Type
RAM	The module stores ephemeral keys/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 keys/SSPs through the memory separation and protection mechanisms. No process other than the module itself can access the keys/SSPs in its process' memory.	dynamic

Table 17 - Storage Areas

9.6 Keys/SSPs Zeroization

Keys and SSPs are explicitly zeroised when the appropriate context object is destroyed or when the system is powered down. Input and output interfaces are inhibited while zeroisation is performed.

10 Self-tests

While the module is executing the self-tests, services are not available, and input and output are inhibited. If the test fails either pre-operational and conditional self-tests, the module reports an error message indicating the cause of the failure and enters the Error State (See section 10.3). The module permits operators to initiate the pre-operational or conditional self-tests for on demand and periodic testing by rebooting the system (i.e., power-cycling).

10.1 Pre-operational Software Integrity Test

The module performs a pre-operational software integrity test 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 Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] with HMAC-SHA256 which is an approved integrity technique.

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA-256	112-bit key	Message Authentication	Software Integrity	Module successful execution	The HMAC value of the runtime image is recalculated and compared with the stored HMAC value pre-computed at compilation time

Table 18 - Preoperational Self-Tests

10.2 Conditional Self-Tests

10.2.1 Conditional Cryptographic Algorithm Self-Tests

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details	Condition
AES-GCM AES-CCM	128-bit key	KAT	CAST	Module becomes operational	Authenticated decryption	Test runs at Power-on before the integrity test
AES-ECB AES-CBC AES-XTS (Testing Revision 2.0)	128-bit key	KAT	CAST	Module becomes operational	Encryption	Test runs at Power-on before the integrity test
AES-ECB AES-CBC	128-bit key	KAT	CAST	Module becomes operational	Decryption	Test runs at Power-on before the integrity test
AES-CCM AES-CMAC	128-bit key	KAT	CAST	Module becomes operational	Authenticated encryption	Test runs at Power-on before the integrity test
CTR_DRBG	AES 128-bit key	KAT	CAST	Module becomes operational	KAT and Health test per SP800-90Arev1 section 11.3	Test runs at Power-on before the integrity test
HMAC-SHA-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

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details	Condition
HMAC-SHA-512	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at Power-on before the integrity test
SHA-1 SHA-256 SHA-512	CAST is covered by higher level HMAC KAT per IG 10.3.B	KAT	CAST	Module becomes operational	Message digest	Test runs at Power-on before the integrity test
RSA Signature Generation	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Signature Generation or Key Generation service request	Test runs at Power-on before the integrity test
RSA Signature Verification	2048-bit modulus with SHA-256	KAT	CAST	Module becomes operational	Signature Verification or Signature Verification or Key Generation service request	Test runs at Power-on before the integrity test
ECDSA Signature Generation	P-224 curve with SHA-224	KAT	CAST	Module becomes operational	Signature Generation or Key Generation service request	Test runs at Power-on before the integrity test
ECDSA Signature Verification	P-224 curve with SHA-224	KAT	CAST	Module becomes operational	Signature Verification or Key Generation service request	Test runs at Power-on before the integrity test
Diffie-Hellman shared secret computation	MODP-2048	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at Power-on before the integrity test
EC Diffie-Hellman shared secret computation	P-224 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at Power-on before the integrity test
PBKDF	SHA-1, SHA-256, SHA-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at Power-on before the integrity test
KBKDF	Counter mode using SHA-1, SHA-256, SHA-512	KAT	CAST	Module becomes operational	Key Derivation	Test runs at Power-on before the integrity test

Table 19 – Conditional Self-Tests

10.2.2 Conditional Pairwise Consistency Test

The Apple corecrypto Module v12.0 [Apple silicon, User, Software, SL1] generates RSA, Diffie-Hellman, EC Diffie-Hellman and ECDSA asymmetric keys and performs a pair-wise consistency tests on the newly generated key pairs.

10.3 Error States

If any of the above-mentioned self-tests described in Sections 10.1, 10.2.1 or 10.2.2 fail, the module reports the cause of the error and enters an error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to power cycle the device which results in the module being reloaded into memory and reperforming the pre-operational self-test and the conditional algorithm self-tests. The module will only enter into the operational state after successfully passing the pre-operational self-test and the conditional self-tests.

State Name	Description	Conditions	Recovery Method	Indicator
Error State	The HMAC-SHA-256 value computed over the module did not match the pre-computed value	Pre-operational Software Integrity Test failure	module reset	Error message "FAILED: fipspost_post_integrity" is sent to the caller
Error State	The computed value in the invoked Conditional CAST did not match the known value	Conditional CAST failure	module reset	Error message "FAILED:<*event*>" sent to the caller (<*event*> refers to any of the cryptographic functions listed in Table 19.)
Error State	The signature failed to verify successfully in the Conditional PCT.	Conditional PCT failure	module reset	Error message "*CCEC_GENERATE_KEY_CONSISTENCY*" returned for EC Error message "*CCRSA_GENERATE_KEY_CONSISTENCY*" returned for RSA Error message "*CCDH_GENERATE_KEY_CONSISTENCY*" returned for DH

Table 20- Error states

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 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 Crypto Officer 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 14 - Non-Approved Services. If the device starts up successfully, then the module has passed all self-tests and is operating in the Approved mode.

The ESV Public Use Document (PUD) reference for physical entropy source is:
https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E14_PublicUse.pdf

The ESV Public Use Document (PUD) reference for non-physical entropy source is:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/15

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

Not Applicable

11.4 Design and Rules

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

- **AES-GCM internal IV** is constructed in compliance with IG C.H scenario 1.

  The GCM IV generation follows RFC 5288 and shall only be used for the TLS protocol version 1.2; thus, the module is compliant with Section 3.3.1 SP 800-52r2. 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 both protocols in case the module’s power is lost and then restored, the key used for the AES GCM encryption/decryption shall be re-distributed. This condition is not enforced by the module; however, it is met implicitly. The module does not retain any state when power is lost. As indicated in Table 11, column Storage, the module exclusively uses volatile storage. This means that AES-GCM key/IVs are not persistently stored during power off: therefore, there is no re-connection possible when the power is back on with re-generation of the key used for GCM. After restoration of the power, the user of the module (e.g., TLS, IKE) along with User application that implements the protocol, must perform a complete new key establishment operation using new random numbers (Entropy input string, DRBG seed, DRBG internal state V and Key, shared secret values that are not retained during power cycle, see table 11) with subsequent KDF operations to establish a new GCM key/IV pair on either side of the network communication channel.

These protocols have not been reviewed or tested by the CAVP and CMVP.

- **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.
- **RSA modulus size (IG C.F)**: In compliance with FIPS 186-4, the RSA signature verification is greater or equal to 1024 bits. All supported RSA modulus sizes have been CAVP tested.
- **Legacy use (IG C.M)**: Per SP800-131r2, the SHA-1 within FIPS 186-4 RSA and ECDSA Digital Signature Verification is used in approved mode (for legacy use), the RSA 1024-bit modulus is used in approved mode for FIPS 186-4 signature verification (for legacy use).
- **PBKDF** see section 9.2
- **KBKDF** see section 9.2

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 binary file listed in section 2.9.

12 Mitigation of other attacks

The module does not claim mitigation of other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CAST	Cryptographic Algorithm Self-Test
CAST5	A symmetric-key 64-bit block cipher with 128-bit key
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ESVP	Entropy Source Validation Program
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAS	Key Agreement Schema
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
KW	AES Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OAEP	Optimal Asymmetric Encryption Padding
OFB	Output Feedback
PAA	Processor Algorithm Acceleration
PBKDF	Password Based Key Derivation Function
PKG	Key-Pair Generation
PKV	Public Key Validation
PRF	Pseudo-Random Function
PSS	Probabilistic Signature Scheme
PUD	Public Use Document
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSC	Shared Secret Computation
TOEPP	Tested Operational Environment Physical Perimeter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS140-3	FIPS PUB 140-3 - Security Requirements for Cryptographic Modules March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
SP 800-140x	CMVP FIPS 140-3 Related Reference https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards
FIPS140-3_IG	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program August 2023 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS140-3_MM	CMVP FIPS 140-3 Draft Management Manual https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/Draft%20FIPS-140-3-CMVP%20Management%20Manual%2009-18-2020.pdf
SP 800-140	FIPS 140-3 Derived Test Requirements (DTR) https://csrc.nist.gov/publications/detail/sp/800-140/final
SP 800-140A	CMVP Documentation Requirements https://csrc.nist.gov/publications/detail/sp/800-140a/final
SP 800-140B	CMVP Security Policy Requirements https://csrc.nist.gov/publications/detail/sp/800-140b/final
SP 800-140C	CMVP Approved Security Functions https://csrc.nist.gov/publications/detail/sp/800-140c/final
SP 800-140D	CMVP Approved Sensitive Security Parameter Generation and Establishment Methods https://csrc.nist.gov/publications/detail/sp/800-140d/final
SP 800-140E	CMVP Approved Authentication Mechanisms https://csrc.nist.gov/publications/detail/sp/800-140e/final
SP 800-140F	CMVP Approved Non-Invasive Attack Mitigation Test Metrics https://csrc.nist.gov/publications/detail/sp/800-140f/final
FIPS180-4	Secure Hash Standard (SHS) March 2012 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-4	Digital Signature Standard (DSS) July 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS197	Advanced Encryption Standard November 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS198-1	The Keyed Hash Message Authentication Code (HMAC) July 2008 http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions August 2015 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
PKCS#1	Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 February 2003 http://www.ietf.org/rfc/rfc3447.txt

RFC3394 Advanced Encryption Standard (AES) Key Wrap Algorithm
September 2002
http://www.ietf.org/rfc/rfc3394.txt

RFC5649 Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm
September 2009
http://www.ietf.org/rfc/rfc5649.txt

SP800-38A NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-38B NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
May 2005
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

SP800-38C NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
May 2004
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

SP800-38D NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
November 2007
http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

SP800-38E NIST Special Publication 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices
January 2010
http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

SP800-38F NIST Special Publication 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
December 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

SP800-38G NIST Special Publication 800-38G - Recommendation for Block Cipher Modes of Operation: Methods for Format - Preserving Encryption
March 2016
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf

SP800-52r2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
August 2019,
https://doi.org/10.6028/NIST.SP.800-52r2

SP800-56Arev3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
April, 2018
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

SP800-56Brev2 Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
March 2019
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

SP800-56Crev2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes
August 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

SP800-57 NIST Special Publication 800-57 Part 1 Revision 5 - Recommendation for Key Management Part 1: General
May 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

SP800-67	NIST Special Publication 800-67 Revision 1 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher January 2012 http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf
SP800-90Arev1	NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-90B	NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
SP800-108r1	NIST Special Publication 800-108r1-upd1 - Recommendation for Key Derivation Using Pseudorandom Functions August 2022 https://doi.org/10.6028/NIST.SP.800-108r1-upd1
SP800-131Arev2	Transitioning the Use of Cryptographic Algorithms and Key Lengths March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
SP800-132	NIST Special Publication 800-132 - Recommendation for Password-Based Key Derivation - Part 1: Storage Applications December 2010 http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
SP800-133rev2	Recommendation for Cryptographic Key Generation June 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP800-135r1	NIST Special Publication 800-135 Revision 1 - Recommendation for Existing Application-Specific Key Derivation Functions December 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SEC	Apple Platform Security https://support.apple.com/guide/security/welcome/web https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
platform certifications	Apple Security Certifications and Compliance Center https://support.apple.com/en-gw/guide/certifications/welcome/web