Apple Inc.

Apple corecrypto Module v14.0 [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

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for Apple corecrypto Module v14.0 [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.

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Apple corecrypto Module v14.0 [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, T2OS, 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.

Tested Operational Environment's Physical Perimeter (TOEPP):

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

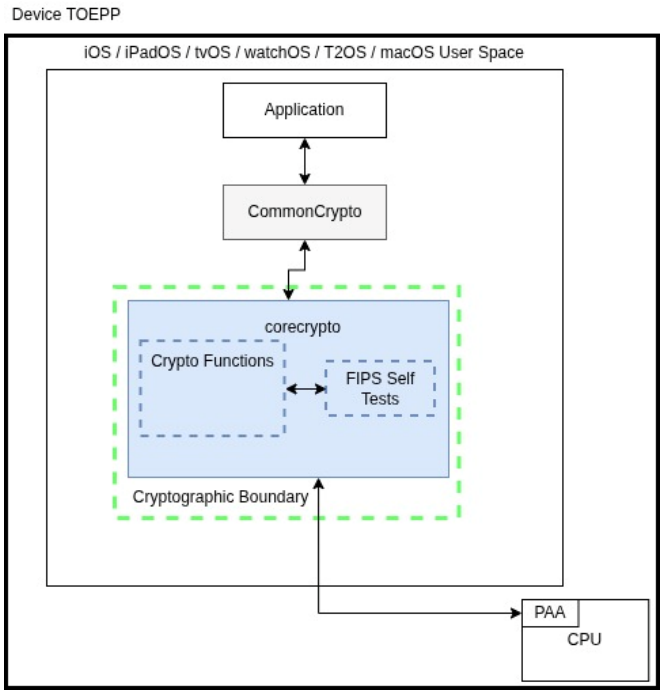

Figure 1: Block Diagram

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-1608.60.11	14.0	N/A	HMAC-SHA256

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
iPadOS 17	iPad (7th generation)	Apple A Series A10 Fusion	Yes	NA	v14.0
iPadOS 17	iPad (7th generation)	Apple A Series A10 Fusion	No	NA	v14.0
iPadOS 17	iPad Pro 10.5-inch	Apple A Series A10X Fusion	Yes	NA	v14.0
iPadOS 17	iPad Pro 10.5-inch	Apple A Series A10X Fusion	No	NA	v14.0
iPadOS 17	iPad mini (5th generation)	Apple A Series A12 Bionic	Yes	NA	v14.0
iPadOS 17	iPad mini (5th generation)	Apple A Series A12 Bionic	No	NA	v14.0
iPadOS 17	iPad Pro 11-inch (2nd generation)	Apple A Series A12Z Bionic	Yes	NA	v14.0
iPadOS 17	iPad Pro 11-inch (2nd generation)	Apple A Series A12Z Bionic	No	NA	v14.0
iPadOS 17	iPad (9th generation)	Apple A Series A13 Bionic	Yes	NA	v14.0
iPadOS 17	iPad (9th generation)	Apple A Series A13 Bionic	No	NA	v14.0
iPadOS 17	iPad Air (4th generation)	Apple A Series A14 Bionic	Yes	NA	v14.0
iPadOS 17	iPad Air (4th generation)	Apple A Series A14 Bionic	No	NA	v14.0
iPadOS 17	iPad mini (6th generation)	Apple A Series A15 Bionic	Yes	NA	v14.0
iPadOS 17	iPad mini (6th generation)	Apple A Series A15 Bionic	No	NA	v14.0
iPadOS 17	iPad Pro 11-inch (3rd generation)	Apple M Series M1	Yes	NA	v14.0
iPadOS 17	iPad Pro 11-inch (3rd generation)	Apple M Series M1	No	NA	v14.0
iPadOS 17	iPad Pro 11-inch (4th generation)	Apple M Series M2	Yes	NA	v14.0
iPadOS 17	iPad Pro 11-inch (4th generation)	Apple M Series M2	No	NA	v14.0
iOS 17	iPhone 11 Pro	Apple A Series A13 Bionic	Yes	NA	v14.0
iOS 17	iPhone 11 Pro	Apple A Series A13 Bionic	No	NA	v14.0
iOS 17	iPhone 12	Apple A Series A14 Bionic	Yes	NA	v14.0
iOS 17	iPhone 12	Apple A Series A14 Bionic	No	NA	v14.0
iOS 17	iPhone 13 Pro Max	Apple A Series A15 Bionic	Yes	NA	v14.0

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
iOS 17	iPhone 13 Pro Max	Apple A Series A15 Bionic	No	NA	v14.0
iOS 17	iPhone 14 Pro Max	Apple A Series A16 Bionic	Yes	NA	v14.0
iOS 17	iPhone 14 Pro Max	Apple A Series A16 Bionic	No	NA	v14.0
watchOS 10	Apple Watch Series S6	Apple S Series S6	Yes	NA	v14.0
watchOS 10	Apple Watch Series S6	Apple S Series S6	No	NA	v14.0
watchOS 10	Apple Watch Series S7	Apple S Series S7	Yes	NA	v14.0
watchOS 10	Apple Watch Series S7	Apple S Series S7	No	NA	v14.0
watchOS 10	Apple Watch Series S8	Apple S Series S8	Yes	NA	v14.0
watchOS 10	Apple Watch Series S8	Apple S Series S8	No	NA	v14.0
tvOS 17	Apple TV 4K (2nd generation)	Apple A Series A12 Bionic	Yes	NA	v14.0
tvOS 17	Apple TV 4K (2nd generation)	Apple A Series A12 Bionic	No	NA	v14.0
tvOS 17	Apple TV 4K (3rd generation)	Apple A Series A15 Bionic	Yes	NA	v14.0
tvOS 17	Apple TV 4K (3rd generation)	Apple A Series A15 Bionic	No	NA	v14.0
T2OS 14	Apple Security Chip T2	Apple T Series T2	Yes	NA	v14.0
T2OS 14	Apple Security Chip T2	Apple T Series T2	No	NA	v14.0
macOS 14	MacBook Air	Apple M Series M1	Yes	NA	v14.0
macOS 14	MacBook Air	Apple M Series M1	No	NA	v14.0
macOS 14	MacBook Pro (14-inch, M1 Pro, 2020)	Apple M Series M1 Pro	Yes	NA	v14.0
macOS 14	MacBook Pro (14-inch, M1 Pro, 2020)	Apple M Series M1 Pro	No	NA	v14.0
macOS 14	MacBook Pro (14-inch, M1 Max, 2021)	Apple M Series M1 Max	Yes	NA	v14.0
macOS 14	MacBook Pro (14-inch, M1 Max, 2021)	Apple M Series M1 Max	No	NA	v14.0
macOS 14	Mac Studio	Apple M Series M1 Ultra	Yes	NA	v14.0
macOS 14	Mac Studio	Apple M Series M1 Ultra	No	NA	v14.0

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
macOS 14	MacBook Pro (13-inch, M2, 2020)	Apple M Series M2	Yes	NA	v14.0
macOS 14	MacBook Pro (13-inch, M2, 2020)	Apple M Series M2	No	NA	v14.0
macOS 14	MacBook Pro (14-inch, M2 Pro, 2023)	Apple M Series M2 Pro	Yes	NA	v14.0
macOS 14	MacBook Pro (14-inch, M2 Pro, 2023)	Apple M Series M2 Pro	No	NA	v14.0
macOS 14	MacBook Pro (14-inch, M2 Max, 2023)	Apple M Series M2 Max	Yes	NA	v14.0
macOS 14	MacBook Pro (14-inch, M2 Max, 2023)	Apple M Series M2 Max	No	NA	v14.0

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

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 Services Table and the Vendor Affirmed Algorithms Table.	Approved	return a '0' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was approved
Non-Approved mode	Non-Approved mode of operation is entered when the module utilizes non-approved security functions in the Non-Approved Services table.	Non-Approved	return any non-zero value from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was non- approved

Table 4: Modes List and Description

Mode Change Instructions and Status

The Module has an Approved and non-Approved mode of operation. The Approved mode of Operation is assumed automatically without any specific configuration. After the device starts up and the module has passed all pre-operational self-tests any calls to the Approved security functions listed in the Approved Services Table will cause the module to implicitly assume the Approved mode of operation and any calls to the non-Approved security functions listed in the Non-Approved Services Table will cause the module to implicitly assume the non-Approved mode of operation. The module transitions back to the approved mode of operation only when an approved service is requested.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5983	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5985	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A5984	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A5986	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A5987	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A5983	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A5986	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5987	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A5983	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A5987	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A5984	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5986	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A5987	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-KW	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-KW	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38F
AES-OFB	A5983	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A5984	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A5986	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A5983	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5984	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A5986	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A5984	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A5986	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A5987	Prediction Resistance - No Mode - AES-128, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A5986	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A5988	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5986	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5988	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5986	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5988	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5986	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5988	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA-1	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-224	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5989	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA2-512/256	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-224	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-256	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-384	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5986	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
HMAC-SHA3-512	A5988	Key Length - Key Length: 8-262144 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5986	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	A5986	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	A5988	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	SP 800-56C Rev. 2
KDF SP800-108	A5986	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KDF SP800-108	A5988	KDF Mode - Counter Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
PBKDF	A5986	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
PBKDF	A5988	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A5986	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA KeyGen (FIPS186-4)	A5988	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A5986	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A5988	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5986	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A5988	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A5986	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	SP 800-56A Rev. 3
SHA-1	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA-1	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-224	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-256	A5989	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-384	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA2-512/256	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 180-4
SHA3-224	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-224	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-256	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-256	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-384	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A5986	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHA3-512	A5988	Message Length - Message Length: 0-32768 Increment 8	FIPS 202
SHAKE-128	A5988	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A5988	Output Length - Output Length: 16-65536 Increment 8	FIPS 202

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	Implemented in compliance with SP800-133rev2 section 4 example 1 and IG D.H

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
ANSI X9.63 KDF	Hash based Key Derivation Function
Blowfish	Encryption / Decryption
CAST5	Encryption / Decryption Key Sizes: 40 to 128 bits in 8-bit increments
DES	Encryption / Decryption Key Size: 56-bits
Diffie-Hellman	Shared Secret Computation using key size < 2048
ECDSA	PKG: Curve P-192; PKV: Curve P-192; compact point representation of points; Signature Generation: Curve P-192 or using MD2, MD4, MD5, RIPEMD, Keccak message digest; Signature Verification: Curve P-192 or using MD2, MD4, MD5, RIPEMD, Keccak message digest
EC Diffie-Hellman	Shared Secret Computation using curves < P-224 or using MD2, MD4, MD5, RIPEMD, Keccak message digest
EdDSA with Ed25519	Key Generation, Signature Generation, Signature Verification, X25519 Key agreement
Integrated Encryption Scheme on elliptic curves	Encryption / Decryption
Keccak	Message Digest
MD2	Message Digest size: 128-bit
MD4	Message Digest size: 128-bit
MD5	Message Digest
OMAC (One-Key CBC MAC)	MAC generation
HMAC	MAC generation using MD2, MD4, MD5, RIPEMD, Keccak message digest
RC2	Encryption / Decryption Key Sizes 8 to 1024-bits
RC4	Encryption / Decryption Key Sizes 8 to 4096-bits
RFC6637	Key Derivation Function
RIPEMD	Message Digest size: 160-bits
RSA Keygen	ANSI X9.31 Key Pair Generation; keys < 2048-bits
RSA Digital Signature	PKCS#1 v1.5 and PSS; Signature Generation Key Size < 2048 or using MD2, MD4, MD5, Keccak, or RIPEMD message digest; Signature Verification Key Size < 1024 or using MD2, MD4, MD5, Keccak, or RIPEMD message digest
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	Hybrid encryption scheme

Name	Use and Function
Encryption) [RFC9180]	
KBKDF	Key derivation using MD2, MD4, MD5, RIPEMD, KECCAK as the underlying PRF
PBKDF	Key derivation using MD2, MD4, MD5, RIPEMD, KECCAK as the underlying PRF
HKDF	Key derivation using MD2, MD4, MD5, RIPEMD, KECCAK as the underlying PRF

Table 7: 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-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,	AES-CBC: (A5983, A5984, A5985, A5986) AES-CFB128: (A5983, A5984, A5986) AES-ECB: (A5983, A5984, A5986, A5987) AES-OFB: (A5983, A5984, A5986) AES-XTS Testing Revision 2.0: (A5983, A5984, A5986) AES-CCM: (A5984, A5986, A5987) AES-CFB8: (A5984, A5986) AES-CTR: (A5984, A5986, A5987) AES-GCM: (A5984, A5986, A5987) AES-KW: (A5984, A5986)

Name	Type	Description	Properties	Algorithms
			192, 256 bits AES-GCM:Key Size / Key Strength: 128, 192, 256 bits AES-KW:Key Size / Key Strength: 128, 192, 256 bits	
Random Number Generation	DRBG	Random Number Generation	Counter DRBG:Key Size/ Key Strength: 128, 256 bits	Counter DRBG: (A5984, A5986, A5987)
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 - 262144 bits; Key Strength: 256 bits HMAC-SHA3-	AES-CMAC: (A5986) HMAC-SHA-1: (A5986, A5988) HMAC-SHA2-224: (A5986, A5988) HMAC-SHA2-256: (A5986, A5988, A5989) HMAC-SHA2-384: (A5986, A5988) HMAC-SHA2-512: (A5986, A5988) HMAC-SHA2-512/256: (A5986, A5988) HMAC-SHA3-224: (A5986, A5988) HMAC-SHA3-256: (A5986, A5988) HMAC-SHA3-384: (A5986, A5988) HMAC-SHA3-512: (A5986, A5988)

Name	Type	Description	Properties	Algorithms
			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 CKG	Asymmetric Key Generation	ECDSA KeyGen (FIPS186-4):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA KeyGen (FIPS186-4):Key Size: 2048, 3072, 4096 bits; Key Strength: from 112 to 150 bits Safe Primes Key Generation:Key Size: 2048, 3072, 4096, 6144, 8192 bits; Key Strength: from 112 to 200 bits	ECDSA KeyGen (FIPS186-4): (A5986, A5988) RSA KeyGen (FIPS186-4): (A5986, A5988) Safe Primes Key Generation: (A5986) CKG: () Key Type: Asymmetric
Asymmetric Key Validation	AsymKeyPair-KeyVer	Asymmetric Key Validation	ECDSA KeyVer (FIPS186-4):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits	ECDSA KeyVer (FIPS186-4): (A5986, A5988)

Name	Type	Description	Properties	Algorithms
Digital Signature Generation	DigSig-SigGen	Digital Signature Generation	ECDSA SigGen (FIPS186-4):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA SigGen (FIPS186-4):Key Size: 2048, 3072, 4096 bits; Key Strength: from 112 to 150 bits EDDSA SigGen:Key Size(Curve): P-224, P-256, P-384, P-521. Key Strength: from 112 to 256 bits	ECDSA SigGen (FIPS186-4): (A5986, A5988) RSA SigGen (FIPS186-4): (A5986, A5988)
Digital Signature Verification	DigSig-SigVer	Digital Signature Verification	ECDSA SigVer (FIPS186-4):Key Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA SigVer (FIPS186-4):Key Size: 1024, 2048, 3072, 4096 bits; Key Strength: from 80 to 150 bits EDDSA SigVer:Key Size(Curve): P-224, P-256, P-384, P-521. Key Strength: from 112 to 256 bits	ECDSA SigVer (FIPS186-4): (A5986, A5988) RSA SigVer (FIPS186-4): (A5986, A5988)
Digital Signature Verification (legacy)	DigSig-SigVer	Digital Signature Verification using SHA-1	Publications:FIPS 140-3 IG C.M legacy algorithms Hashes:SHA-1 ECDSA SigVer (FIPS186-4):Key	ECDSA SigVer (FIPS186-4): (A5986, A5988) RSA SigVer (FIPS186-4): (A5986, A5988)

Name	Type	Description	Properties	Algorithms
			Size(Curve): P-224, P-256, P-384, P-521; Key Strength: from 112 to 256 bits RSA SigVer (FIPS186-4):Key Size: 1024, 2048, 3072, 4096 bits; Key Strength: from 80 to 150 bits	SHA-1: (A5986, A5988)
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: (A5986) KAS-FFC-SSC Sp800-56Ar3: (A5986)
Key Derivation	KAS-56CKDF KBKDF PBKDF	Key Derivation	KDF SP800-108:Key Size / Key Strength: 128, 192, 256 bits; Supported Lengths: 8-4096 Increment 8; Fixed Data Order: Before Fixed Data; Counter Length: 8, 16, 24, 32 PBKDF:Key Size: 128 - 262144; Key Strength: 128 - 256; Password length: 8- 128 bytes Increment 1; Salt Length: 128-4096 Increment 8;	KDF SP800-108: (A5986, A5988) PBKDF: (A5986, A5988) KDA HKDF SP800-56Cr2: (A5988)

Name	Type	Description	Properties	Algorithms
			Iteration Count: 10-1000 Increment 1	
Message Digest	SHA	Message Digest	SHA-1:N/A SHA2-224:N/A SHA2-256:N/A SHA2-384:N/A SHA2-512:N/A SHA2-512/256:N/A SHA3-224:N/A SHA3-256:N/A SHA3-384:N/A SHA3-512:N/A	SHA-1: (A5986, A5988) SHA2-224: (A5986, A5988) SHA2-256: (A5986, A5988, A5989) SHA2-384: (A5986, A5988) SHA2-512: (A5986, A5988) SHA2-512/256: (A5986, A5988) SHA3-224: (A5986, A5988) SHA3-256: (A5986, A5988) SHA3-384: (A5986, A5988) SHA3-512: (A5986, A5988) SHAKE-128: (A5988) SHAKE-256: (A5988)

Table 8: 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 following 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 following RFC 4106 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 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. 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, every RSA modulus size used by the cryptographic module has been validated by the CAVP. The respective certificates are listed in the Approved Algorithms Table of this security policy. There are no untested RSA modulus sizes used by the cryptographic module.

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.

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.

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. SHA-1 used in the context of ECDSA SigVer and RSA SigVer, is allowed for Legacy use only.

2.8 RBG and Entropy

Cert Number	Vendor Name
E113	apple

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Apple corecrypto physical entropy source	Physical	See Tested Operational Environment Table in section 2.2	256 bit	Full Entropy	SHA-256 [ACVP cert. #C1223]

Table 10: 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 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 asymmetric key generation in compliance with SP800-133rev2 section 4 example 1 and IG D.H.

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).

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 11: Ports and Interfaces

The module does not implement a Control Output Logical Interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

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 12: 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	Symmetric Encryption and Decryption	Crypto Officer - AES key: W,E Unauthenticated
Secure Hash Generation	Generate a digest for the requested algorithm	0	message	digest	Message Digest	Crypto Officer Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Authentication Generation	Generate a MAC digest using the requested SHA algorithm or AES algorithm	0	message, MAC key, MAC algorithm	MAC	Message authentication (MAC)	Crypto Officer - AES key: W,E - HMAC key: W,E Unauthenticated
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 Unauthenticated
RSA signature generation and verification	Sign a message with a specified RSA private key. Verify the signature of a message with a specified RSA public key.	0	SigGen: private key, message, hash function; SigVer: public key, digital signature, message, hash function	SigGen: computed signature; SigVer: pass/fail result of digital signature verification	Digital Signature Generation Digital Signature Verification Digital Signature Verification (legacy)	Crypto Officer - RSA key pair: W,E Unauthenticated
ECDSA signature generation and verification	Sign a message with a specified ECDSA private key Verify the signature of a message with a specified	0	SigGen: private key, message, hash function; SigVer: public key, digital signature, messag	SigGen: computed signature; SigVer: pass/fail result of digital signature verification	Digital Signature Generation Digital Signature Verification Digital Signature Verification (legacy)	Crypto Officer - ECDSA key pair: W,E Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ECDSA public key		e, hash function			
Random Number Generation	Generate random number	0	requested number of bits	random bit-string	Random Number Generation	Crypto Officer - Entropy input string: E - DRBG seed, internal state V value, and key (IG D.L compliant): G,W,E Unauthenticated
PBKDF	Derive key from password	0	Password	PBKDF derived key	Key Derivation	Crypto Officer - PBKDF derived key: G,R - PBKDF password: W,E Unauthenticated
KBKDF	Derive key from key derivation key	0	KBKDF key derivation key	KBKDF derived key	Key Derivation	Crypto Officer - KBKDF key derivation key: W,E - KBKDF derived key: G,R Unauthenticated
RSA key pair generation	Generate a keypair for a requested modulus	0	key size	key pair	Asymmetric Key Generation	Crypto Officer - DRBG seed, internal state V value, and key (IG D.L compliant): W,E - RSA key

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			key and possessed private key			- EC Diffie-Hellman shared secret: G,R Unauthenticated
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 Random Number Generation Message authentication (MAC) Asymmetric Key Generation Asymmetric Key Validation Digital Signature Generation Digital Signature Verification Digital Signature Verification (legacy) Shared Secret Computation Key Derivation Message Digest	Crypto Officer Unauthenticated
Show Status	Return the module status	N/A	N/A	Status output	None	Crypto Officer Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show module and version info	Return Module Base Name and Module Version Number	N/A	N/A	Module information	None	Crypto Officer Unauthenticated
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 of asymmetric crypto function context and all resources of key derivation	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 key: Z - KBKDF key derivation key: Z - PBKDF password: Z - Diffie-Hellman key pair: Z - EC Diffie Hellman key pair: Z - Diffie-Hellman shared secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	function context are released					- EC Diffie-Hellman shared secret: Z Unauthenticated

Table 13: 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 or using MD2, MD4, MD5, Keccak, or RIPEMD message digest; Signature Verification: Curve P-192 or using MD2, MD4, MD5, Keccak, or RIPEMD message digest	ECDSA	CO
EC Diffie-Hellman	Shared Secret Computation using curves < P-224 or using MD2, MD4, MD5, Keccak, or RIPEMD message digest	EC Diffie-Hellman	CO
EdDSA with Ed25519	Key Generation, Signature Generation, Signature Verification, Key agreement	EdDSA with Ed25519	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
MD5	Message Digest	MD5	CO
OMAC (One-Key CBC MAC)	MAC generation	OMAC (One-Key CBC MAC)	CO
HMAC (using non-approved digest)	MAC generation using MD2, MD4, MD5, RIPEMD, Keccak message digest	HMAC	CO
RC2	Encryption / Decryption Key Sizes 8 to 1024-bits	RC2	CO

Name	Description	Algorithms	Role
RC4	Encryption / Decryption Key Sizes 8 to 4096-bits	RC4	CO
RFC6637	Key Derivation Function	RFC6637	CO
PBKDF (using non-approved PRF)	Password-based Key Derivation Function using MD2, MD4, MD5, RIPEMD, Keccak	PBKDF	CO
KBKDF (using non-approved PRF)	Key-based Key Derivation Function using MD2, MD4, MD5, RIPEMD, Keccak	KBKDF	CO
HKDF (using non-approved PRF)	HKDF using MD2, MD4, MD5, RIPEMD, Keccak	HKDF	CO
RIPEMD	Message Digest size: 160-bits	RIPEMD	CO
RSA Keygen	ANSI X9.31 Key Pair Generation; keys < 2048-bits	RSA Keygen	CO
RSA Digital Signature	PKCS#1 v1.5 and PSS; Signature Generation Key Size < 2048 or using MD2, MD4, MD5, RIPEMD, Keccak; Signature Verification Key Size < 1024 or using MD2, MD4, MD5, RIPEMD, Keccak	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
Keccak	Message Digest	Keccak	CO

Table 14: Non-Approved Services

4.5 External Software/Firmware Loaded

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

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. Integrity tests on demand is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

6.2 Configuration Settings and Restrictions

The module is supplied as part of Device OS, a commercially available general-purpose operating system executing on the computing platforms specified in section 2.2.

7 Physical Security

The FIPS 140-3 physical security requirements do not apply to the Apple corecrypto Module v14.0 [Apple silicon, User, Software, SL1] since it is a software module.

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.

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 15: 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 16: 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	Invocation of zeroization function cc_clear
Power down	SSPs are zeroised when the system is powered down	SSPs are zeroised when the system is powered down	Operator can initiate power down
Intermediate value zeroization	Intermediate keygen values are zeroized before the	Intermediate keygen values are zeroized before the	N/A

Zeroization Method	Description	Rationale	Operator Initiation
	module returns from the key generation function.	module returns from the key generation function.	

Table 17: 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			Symmetric Encryption and Decryption
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 Digital Signature Verification (legacy)
RSA key pair	RSA key pair (including intermediate keygen values)	2048 - 4096 - 112 to 150 bits	Asymmetric - CSP	Asymmetric Key Generation		Digital Signature Generation Digital Signature Verification Digital

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Signature Verification (legacy)
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 password	PBKDF password	64 to 1024 bits - N/A	Password - CSP			Key Derivation
KBKDF key derivation key	KBKDF key derivation key	128 to 256 bits - 128 to 256 bits	Derivation key - CSP			Key Derivation
KBKDF derived key	KBKDF derived key	128 to 256 bits - 128 to 256 bits	Derived key - CSP	Key Derivation		
Diffie-Hellman key pair	Diffie-Hellman key pair (including intermediate keygen values)	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits	Asymmetric - CSP	Asymmetric Key Generation		Shared Secret Computation
Diffie-Hellman	Diffie-Hellman	MODP-2048,	Asymmetric - CSP		Shared Secret	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
shared secret	shared secret	MODP-3072, MODP-4096, MODP-6144, MODP-8192 - 112 to 200 bits			Computation	
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		Shared Secret Computation
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	

Table 18: 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	RAM:Plaintext	From service	Context object	DRBG seed, internal state V value, and

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	API output parameters		invocation to service completion	destruction Power down Intermediate value zeroization	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
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

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

Table 19: 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.

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 20: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt	128-bit key encrypt	KAT	CAST	Module becomes operational	Symmetric encrypt	Test runs at power-on before the integrity test
AES-ECB Decrypt	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric decryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 Encrypt	128-bit key encrypt	KAT	CAST	Module becomes operational	Symmetric encryption	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 Decrypt	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric decryption	Test runs at power-on before the integrity test

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
Counter DRBG	128-bit key	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
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-SHA3-512	SHA3-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
RSA KeyGen	PCT with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
RSA SigGen	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
RSA SigVer	PKCS#1 v1.5 with 2048 bit key and SHA2-256	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
ECDSA KeyGen	PCT with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA KeyVer	PCT with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen	P-224 with SHA-224	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer	P-224 with SHA-224	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
KAS-ECC-SSC Sp800-56Ar3 (A5986)	P-224 curve	KAT	CAST	Module becomes operational	Shared secret computation	Test runs at power-on before the integrity test
KAS-FFC-SSC Sp800-56Ar3 (A5986)	MODP-2048	PCT	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	Password-based key derivation	Test runs at power-on before the integrity test
KDF SP800-108	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	KAT	CAST	Module becomes operational	Key-based key derivation	Test runs at power-on before the integrity test
KDA HKDF SP800-56Cr2	HMAC algorithm: SHA-1, SHA2-256, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512. with 256-bit secret	KAT	CAST	Module becomes operational	Hash-based key derivation	Test runs at power-on before the integrity test
Safe Prime Key Generation	MODP-2048	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation

Table 21: 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 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt	KAT	CAST	On Demand	Manually
AES-ECB Decrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 Encrypt	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 Decrypt	KAT	CAST	On Demand	Manually
AES-GCM Encrypt	KAT	CAST	On Demand	Manually
AES-GCM Decrypt	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-SHA3-512	KAT	CAST	On Demand	Manually
RSA KeyGen	PCT	PCT	On Demand	Manually
RSA SigGen	KAT	CAST	On Demand	Manually
RSA SigVer	KAT	CAST	On Demand	Manually
ECDSA KeyGen	PCT	PCT	On Demand	Manually
ECDSA KeyVer	PCT	PCT	On Demand	Manually
ECDSA SigGen	KAT	CAST	On Demand	Manually
ECDSA SigVer	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5986)	KAT	CAST	On Demand	Manually
KAS-FFC-SSC Sp800-56Ar3 (A5986)	PCT	CAST	On Demand	Manually
PBKDF	KAT	CAST	On Demand	Manually
KDF SP800-108	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA HKDF SP800-56Cr2	KAT	CAST	On Demand	Manually
Safe Prime Key Generation	PCT	PCT	On Demand	Manually

Table 23: Conditional Periodic Information

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" send to caller or 2) Error message "FAILED:<event>" sent to caller (<event> refers to any of the cryptographic functions listed Table - Conditional Self-Tests 3) Error code "CCEC_GENERATE_KEY_CONSISTENCY" returned for ECDSA and EC Diffie-Hellman Error code "CCRSA_GENERATE_KEY_CONSISTENCY" returned for RSA Error code "CCDH_GENERATE_KEY_CONSISTENCY" returned for Diffie-Hellman

Table 24: 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).

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.

The administrator should request the "Show module and version info" service from the module and confirm that it outputs "Apple corecrypto Module v14.0 [Apple ARM, User, Software, SL1]" to identify the module and its version. The term Apple ARM identifies Apple Silicon chips

Apple Platform Certifications guide (platform certifications) and Apple Platform Security guide (SEC) are provided by Apple which offers IT System Administrators with the necessary technical information to ensure FIPS 140-3 Compliance of the deployed systems. This guide walks the reader through the system's assertion of cryptographic module integrity and the steps necessary if module integrity requires remediation.

11.3 Non-Administrator Guidance

None.

11.4 Design and Rules

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

- AES-GCM see section 2.7.
- AES-XTS see section 2.7.
- PBKDF see section 2.7.
- RSA see section 2.7.

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 Table 2.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.