Apple Inc.

Apple corecrypto Module v14.1 [Apple silicon, Kernel, 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
www.atsec.com

Table of Contents

List of Tables

List of Figures

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.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for Apple corecrypto Module v14.1 [Apple silicon, Kernel, 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 800-140Br1.

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 v14.1 [Apple silicon, Kernel, Software, SL1] cryptographic module (hereafter referred to as “the module”) provides implementations of low-level cryptographic primitives to the visionOS’s kernels Security Framework and Common Crypto. The module provides services intended to protect data in transit and at rest.

The module is optimized for library use within the visionOS kernel space and does not contain any terminating assertions or exceptions. It is implemented as a visionOS dynamically loadable library. The library is loaded into the visionOS kernel and its cryptographic functions are made available to visionOS kernel services only.

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

Module Type: Software

Module Embodiment: MultiChipStand

Cryptographic Boundary: The module cryptographic boundary is delineated by the dotted green rectangle in the Figure 1 where the Kernel Extension (KEXT) is a bundle that performs low-level tasks. KEXTs run in kernel space, which gives them elevated privileges and the ability to perform tasks that user-space apps can’t.

Tested Operational Environment’s Physical Perimeter (TOEPP): The physical perimeter is represented by the most exterior black line in the block diagram Figure 1. The module executes within the kernel space of the computing platforms and operating systems listed in the Tested Operational Environments Table section 2.2.

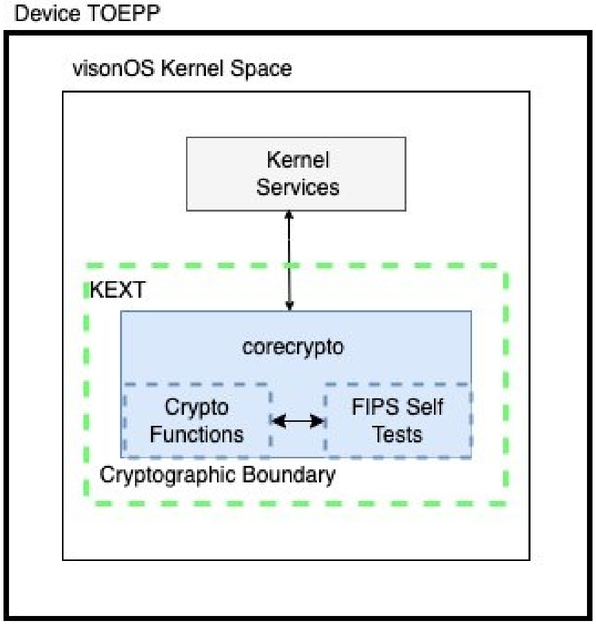

Figure 1: Block Diagram

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-1638.100.62	14.1	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)
visionOS 1	Apple Vision Pro	Apple M Series (ARMv8.6-A) M2	Yes	NA	14.1
visionOS 1	Apple Vision Pro	Apple M Series (ARMv8.6-A) M2	No	NA	14.1

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

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

N/A for this module.

2.3 Excluded Components

None for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Approved mode of operation is entered when the module utilizes the services that use the security functions listed in the Approved Algorithms Table and the Vendor Affirmed Algorithms Table.	Approved	return a '1' from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was approved
Non-Approved mode	Non-Approved mode of operation is entered when the module utilizes non-approved security functions in the Table Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.	Non-Approved	return any non-zero value from fips_allowed_mode() for block cipher functions and fips_allowed() for all other services to indicate the executed cryptographic algorithm was non- approved

Table 4: Modes List and Description

2.4.1 Mode Change Instructions and Status

The Module has an Approved and non-Approved mode of operation. The Approved mode of Operation is assumed automatically without any specific configuration. If the device starts up successfully then the module has passed all self-tests and is operating in the Approved mode. Any calls to the non-Approved security functions listed in the Non-Approved Services Table will cause the module to assume the non-Approved mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5413	-	SP 800-38A
AES-CBC	A5414	-	SP 800-38A
AES-CCM	A5416	-	SP 800-38C
AES-CFB128	A5413	-	SP 800-38A
AES-CFB128	A5414	-	SP 800-38A
AES-CFB8	A5414	-	SP 800-38A
AES-CTR	A5414	-	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A5416	-	SP 800-38A
AES-ECB	A5413	-	SP 800-38A
AES-ECB	A5414	-	SP 800-38A
AES-ECB	A5416	-	SP 800-38A
AES-GCM	A5416	-	SP 800-38D
AES-KW	A5414	-	SP 800-38F
AES-OFB	A5413	-	SP 800-38A
AES-OFB	A5414	-	SP 800-38A
AES-XTS Testing Revision 2.0	A5413	-	SP 800-38E
Counter DRBG	A5414	-	SP 800-90A Rev. 1
Counter DRBG	A5416	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A5369	-	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A5369	-	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A5369	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A5369	-	FIPS 186-4
HMAC-SHA-1	A5369	-	FIPS 198-1
HMAC-SHA2-224	A5369	-	FIPS 198-1
HMAC-SHA2-256	A5369	-	FIPS 198-1
HMAC-SHA2-256	A5417	-	FIPS 198-1
HMAC-SHA2-384	A5369	-	FIPS 198-1
HMAC-SHA2-384	A5415	-	FIPS 198-1
HMAC-SHA2-512	A5369	-	FIPS 198-1
HMAC-SHA2-512	A5415	-	FIPS 198-1
HMAC-SHA2-512/256	A5369	-	FIPS 198-1
HMAC-SHA2-512/256	A5415	-	FIPS 198-1
RSA SigGen (FIPS186-4)	A5369	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A5369	-	FIPS 186-4
SHA-1	A5369	-	FIPS 180-4
SHA2-224	A5369	-	FIPS 180-4
SHA2-256	A5369	-	FIPS 180-4
SHA2-256	A5417	-	FIPS 180-4
SHA2-384	A5369	-	FIPS 180-4
SHA2-384	A5415	-	FIPS 180-4
SHA2-512	A5369	-	FIPS 180-4
SHA2-512	A5415	-	FIPS 180-4
SHA2-512/256	A5369	-	FIPS 180-4
SHA2-512/256	A5415	-	FIPS 180-4

Table 5: Approved Algorithms

The FIPS 186-4 CAVP tests in the listed ACVP certificates above are mathematically identical to the FIPS 186-5 CAVP tests. Per FIPS 140-3 C.K Additional Comments 2, the module claims compliance with FIPS 186-5 tests.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric (CKG)		N/A	SP 800-133Rev2 section 4 example 1

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
DES	Encryption / Decryption
ECDSA	PKG: Curve P-192; PKV: Curve P-192; Signature Generation: Curve P-192; Signature Verification: Curve P-192
ECDSA KeyGen	Key Pair Generation for compact point representation of points
EdDSA	Key Generation, Signature Generation, Signature Verification with Ed25519
HKDF [SP800-56Crev2]	Key Derivation Function
Integrated Encryption Scheme on elliptic curves (ECIES)	Encryption / Decryption
MD2	Message Digest
MD4	Message Digest
OMAC (One-Key CBC MAC)	MAC generation /verification
RC2	Encryption / Decryption
RC4	Encryption / Decryption
RIPEMD	Message Digest
RSA SigGen	PKCS#1 v1.5 and PSS; Signature Generation using key sizes less than 2048-bits
RSA SigVer	Signature Verification using key sizes less than1024
RSA Key Wrapping	OAEP, PKCS#1 v1.5 and -PSS schemes
Triple-DES [SP 800-67r2]	Encryption / Decryption
MD5	Message Digest
RFC 6637 Key Derivation	Key Derivation Function

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 Length: 128, 192, 256 AES-CCM:Key Length: 128, 192, 256 AES-CFB128:Key Length: 128, 192, 256 AES-CFB8:Key Length: 128, 192, 256 AES-CTR:Key Length: 128, 192,	AES-CBC: (A5413, A5414) AES-CCM: (A5416) AES-CFB128: (A5413, A5414) AES-CFB8: (A5414) AES-CTR: (A5414, A5416) AES-ECB: (A5413, A5414, A5416) AES-GCM: (A5416) AES-OFB: (A5413, A5414) AES-XTS Testing

Name	Type	Description	Properties	Algorithms
			256 AES-ECB:Key Length: 128, 192, 256 AES-GCM:Key Length: 128, 192, 256 AES-OFB:Key Length: 128, 192, 256 AES-XTS:Key Length: 128, 256	Revision 2.0: (A5413)
Key Wrapping and Unwrapping	KTS-Wrap BC-Auth	Key Wrapping and Unwrapping	AES-KW:Key Length: 128, 192, 256	AES-KW: (A5414)
Random Number Generation	DRBG	Random Number Generation	Counter DRBG:AES-128, AES-256; Derivation Function Enabled; No Prediction Resistance; Key size: 128, 256 bits	Counter DRBG: (A5414, A5416)
Keyed Hash	MAC	Keyed Hash	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-SHA2-256: (A5417, A5369) HMAC-SHA2-384: (A5415, A5369) HMAC-SHA2-512: (A5415, A5369) HMAC-SHA2-512/256: (A5415, A5369) HMAC-SHA-1: (A5369) HMAC-SHA2-224: (A5369)
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	ECDSA KeyGen (FIPS186-4): (A5369) Asymmetric (CKG): ()
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): (A5369)

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	ECDSA SigGen (FIPS186-4): (A5369) RSA SigGen (FIPS186-4): (A5369)
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	ECDSA SigVer (FIPS186-4): (A5369) RSA SigVer (FIPS186-4): (A5369)
Digital Signature Verification (Legacy)	DigSig-SigVer	Digital Signature Verification using SHA1	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	ECDSA SigVer (FIPS186-4): (A5369) RSA SigVer (FIPS186-4): (A5369)
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	SHA2-384: (A5415, A5369) SHA2-512: (A5415, A5369) SHA2-512/256: (A5415, A5369) SHA2-256: (A5417, A5369) SHA-1: (A5369) SHA2-224: (A5369)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM

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

The GCM IV generation follows RFC 4106 and shall only be used for the IPsec protocol version 3. When the IV in RFC 4106 exhausts the maximum number of possible values for a given security association, either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES-GCM encryption keys are derived.

In compliance with IG C.H section 3, if the module's power is lost and then restored, the key used for the AES GCM encryption/decryption shall be re-distributed. This condition is not enforced by the module.

AES-XTS

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

SHA-1:

Digital signature generation using SHA-1 is non-approved and not allowed in approved services. Digital signature verification using SHA-1 is considered approved ("Legacy"). HMAC using SHA-1 is approved.

The SHA-1 algorithm, as implemented by the module, will be non-approved for all purposes except signature verification, starting January 1, 2031.

Note: 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.

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	256 bit	SHA-256 [ACVP cert. #C1223]

Table 10: Entropy Sources

Entropy source(s): The random bits used to seed and reseed the module's approved DRBG comes from a physical entropy source residing within the TOEPP. The entropy source includes a vetted conditioning component in the form of a SHA-256. The min-entropy rate at the output of the entropy source (h_out for the output of the conditioning component per Section 3.1.5 of SP 800-90B) is 256 bits per 256-bit output.

The entropy source follows IG 9.3.A scenario 1.(b) i.e., the module is a software module and the entropy sources reside outside of the cryptographic boundary but inside the module's TOEPP.

DRBG(s): The module implements an SP 800-90ARev1 approved deterministic random bit generator (DRBG) in the form of a CTR_DRBG using AES-256 with derivation function and without prediction resistance.

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

DRBG Output: The output of CTR_DRBG provides up to 256-bits of security strength.

2.9 Key Generation

The module implements asymmetric key generation compliant to SP800-133r2 Section 4 examples 1 and is listed as a vendor affirmed algorithm per FIPS 140_3 IG D.H. The seed material used to generate the asymmetric key pairs is provided directly output from the module's CTR_DRBG.

The module does not implement symmetric key generation.

2.10 Key Establishment

The module does not implement key establishment.

2.11 Industry Protocols

No parts of the IPSec, 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 Output	Data inputs/outputs are provided in the variables passed in the C language Kernel Interfaces (KPIs) 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 KPI lists possible return codes. A complete list of all return codes returned by the C language KPIs within the module is provided in the header files and the KPI documentation. Messages are also documented in the KPI documentation.

Table 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 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	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
AES Key Wrapping / Key Unwrapping	Execute AES-key wrapping or unwrapping operation	0	key wrapping key, unwrapped key / Wrapped key, AES key wrapping key	wrapped key / unwrapped key	Key Wrapping and Unwrapping	Crypto Officer - AES key-wrapping key: W,E
Secure Hash Generation	Generate a digest for the requested algorithm	0	message	digest	Message Digest	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Message Authentication Generation	Generate a MAC digest using the requested SHA algorithm	0	message, MAC key, MAC algorithm	MAC	Keyed Hash	Crypto Officer - HMAC key: W,E
Message Authentication Code Verification	Verify a MAC digest	0	MAC, message, MAC key, MAC algorithm	pass/fail	Keyed Hash	Crypto Officer - HMAC key: W,E
RSA signature generation and verification	Sign a message with a specified RSA private key. Verify the signature of a message with a specified RSA 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
ECDSA signature generation and verification	Sign a message with a specified ECDSA private key Verify the signature of a message with a specified ECDSA public key	0	SigGen: private key, message, hash function; SigVer: public key, digital signature, message, hash function	SigGen: computed signature; SigVer: pass/fail result of digital signature verification	Digital Signature Generation Digital Signature Verification Digital Signature Verification (Legacy)	Crypto Officer - ECDSA key pair: W,E
Random Number Generation	Generate random number	0	length of generated number	random bit-string	Random Number Generation	Crypto Officer - Entropy input string: E - DRBG seed, internal state V value, and key: G,W,E
ECDSA key pair generation and validation	Generate a keypair for a requested elliptic curve and validity	0	curve size	key pair	Asymmetric Key Generation Asymmetric Key Validation	Crypto Officer - DRBG seed, internal state V value, and key: W,E - ECDSA key pair: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-test	execute CASTs	0	power	pass/fail results	Symmetric Encryption and Decryption Key Wrapping and Unwrapping Random Number Generation Keyed Hash Asymmetric Key Generation Asymmetric Key Validation Digital Signature Generation Digital Signature Verification Digital Signature Verification (Legacy) Message Digest	Crypto Officer
Show Status	Return the module status	N/A	N/A	Status output	None	Crypto Officer
Show version/module info	Return Module Base Name and Module Version Number	N/A	N/A	Module information	None	Crypto Officer
Zeroization	SSPs are zeroised when the system is powered down, when all resources of symmetric crypto function context, all resources of hash context, all resources of asymmetric crypto function context are released.	0	N/A	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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						value, and key: Z

Table 13: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Triple-DES encryption / decryption	Execute Triple-DES mode encrypt or decrypt operation.	Triple-DES [SP 800-67r2]	CO
RSA Key Encapsulation	The CAST does not perform the full KTS, only the raw RSA encrypt/decrypt.	RSA Key Wrapping	CO
RSA Signature Generation	Sign a message with a non-approved RSA private key size	RSA SigGen	CO
RSA Signature Verification	Verify the signature of a message with a non-approved RSA public key size	RSA SigVer	CO
ECDSA key-pair generation, ECDSA signature generation, ECDSA signature verification	For curve P-192	ECDSA	CO
ECDSA Key Pair Generation for compact point representation of points	For compact point representation of points	ECDSA KeyGen	CO
EdDSA Key Generation, Signature Generation, Signature Verification	Ed25519	EdDSA	CO
ECIES	Elliptic Curve encrypt/ decrypt	Integrated Encryption Scheme on elliptic curves (ECIES)	CO
ANSI X9.63 Key Derivation	SHA-1 hash-based	ANSI X9.63 KDF	CO
SP800-56Crev2 Key Derivation (HKDF)	SHA-256 hash-based	HKDF [SP800-56Crev2]	CO
OMAC Message Authentication Code Generation	One-Key CBC-MAC using 128-bit key	OMAC (One-Key CBC MAC)	CO
OMAC Message Authentication Code Verification	One-Key CBC-MAC using 128-bit key	OMAC (One-Key CBC MAC)	CO
Message digest generation	Message digest generation using non-approved algorithms	MD2 MD4 RIPEMD MD5	CO
Symmetric encryption / decryption	Symmetric encryption / decryption using non-approved algorithms	Blowfish CAST5 DES RC2 RC4	CO
RFC 6637 KDF	SHA-256, SHA-512, AES-128, AES-256	RFC 6637 Key Derivation	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 test on demand is performed as part of the Pre-Operational Self-Tests, 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 visionOS, 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 v14.1 [Apple silicon, Kernel, 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	Temporary storage for SSPs used by the module as part of service execution. The module does not perform persistent storage of SSPs	Dynamic

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
KPI input parameters	Operator calling application (TOEPP)	Cryptographic module	Plaintext	Manual	Electronic	
KPI 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
Wipe and Free memory block allocated	Zeroizes the SSPs contained within the cipher handle.	Memory occupied by SSPs is overwritten with zeroes and then it is released, which renders the SSP values irretrievable. The completion of the zeroization routine indicates that the zeroization procedure succeeded.	By calling the cipher related zeroization API
Module Reset	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	By unloading and reloading the module
Intermediate value zeroization	Intermediate keygen values are zeroized before the module returns from the key generation function.	Intermediate keygen values are zeroized before the module returns from the key generation function.	N/A

Table 17: SSP Zeroization Methods

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key-wrapping key	AES KW	128 to 256 bits - 128 to 256 bits	symmetric - CSP			Key Wrapping and Unwrapping
HMAC key	HMAC key	128 to 256 - 128 to 256	MAC - CSP			Keyed Hash
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		Asymmetric Key Validation 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			Digital Signature Generation Digital Signature Verification Digital Signature Verification (Legacy)
Entropy input string	Entropy input string	256 bits - 256 bits	Entropy input string - CSP			Random Number Generation
DRBG seed, internal state V value, and key	DRBG input parameters	256 bits - 256 bits	DRBG - CSP	Random Number Generation		Random Number Generation

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
AES key-wrapping key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
HMAC key	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset	
ECDSA key pair	KPI input parameters KPI output parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset Intermediate	DRBG seed, internal state V value, and key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				value zeroization	
RSA key pair	KPI input parameters	RAM:Plaintext	From service invocation to service completion	Wipe and Free memory block allocated Module Reset 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	Module Reset	DRBG seed, internal state V value, and key:Used With
DRBG seed, internal state V value, and key			Storage duration during the usage of the CSP	Module Reset	Entropy input string:Used With

Table 19: SSP Table 2

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 (A3687)	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-GCM (A5416)	128-bit key, encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
Counter DRBG (A5414)	128-bit key	KAT	CAST	Module becomes operational	Compliant with SP 800-90Ar1	Test runs at power-on before the integrity test
Counter DRBG (A5416)	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 (A5417)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-256 (A5369)	SHA2-256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA-1 (A5369)	SHA-1	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5415)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512 (A5369)	SHA2-512	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A5369)	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 (FIPS186-4) (A5369)	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 (FIPS186-4) (A5369)	PCT with SHA2-256	PCT	PCT	Successful key pair generation	Signature generation & verification	Key pair generation
ECDSA SigGen (FIPS186-4) (A5369)	P-224 with SHA-224	KAT	CAST	Module becomes operational	Digital signature generation	Test runs at power-on before the integrity test
ECDSA SigVer (FIPS186-4) (A5369)	P-224 with SHA-224	KAT	CAST	Module becomes operational	Digital signature verification	Test runs at power-on before the integrity test
AES-CBC (A5413)	128-bit key encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-CBC (A5414)	128-bit key encrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5413)	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5414)	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-ECB (A5416)	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
AES-XTS Testing Revision 2.0 (A5413)	128-bit key decrypt	KAT	CAST	Module becomes operational	Symmetric operation	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A5415)	SHA2-512/256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test
HMAC-SHA2-512/256 (A5369)	SHA2-512/256	KAT	CAST	Module becomes operational	Message authentication	Test runs at power-on before the integrity test

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A3687)	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-GCM (A5416)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A5414)	KAT	CAST	On Demand	Manually
Counter DRBG (A5416)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5417)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A5369)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A5369)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5415)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A5369)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A5369)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-4) (A5369)	KAT	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-4) (A5369)	PCT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-4) (A5369)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-4) (A5369)	KAT	CAST	On Demand	Manually
AES-CBC (A5413)	KAT	CAST	On Demand	Manually
AES-CBC (A5414)	KAT	CAST	On Demand	Manually
AES-ECB (A5413)	KAT	CAST	On Demand	Manually
AES-ECB (A5414)	KAT	CAST	On Demand	Manually
AES-ECB (A5416)	KAT	CAST	On Demand	Manually
AES-XTS Testing Revision 2.0 (A5413)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A5415)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512/256 (A5369)	KAT	CAST	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	1) Pre-operational Software Integrity Test failure or 2) Conditional CAST failure 3)	Power cycle the device which results in the module being reloaded into memory and reperforming	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

Name	Description	Conditions	Recovery Method	Indicator
	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	Conditional PCT failure	the pre-operational software integrity test and the Conditional CASTs.	

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 visionOS defined in section 2 and delivered/ installed with the respective visionOS. 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 visionOS version. For additional assurance, the module is digitally signed by vendor, and it is verified during the integration into Host visionOS.

This digital signature-based integrity protection during the delivery/integration process is not to be confused with the HMAC-256 based integrity check performed by the module itself as part of its pre-operational self- tests.

11.2 Administrator Guidance

The Approved mode of operation is configured in the system by default and can only be transitioned into the non-Approved mode by calling one of the non-Approved services listed in Table - Non-Approved Services. If the device starts up successfully, then the module has passed all self-tests and is operating in the Approved mode.

Apple Platform Certifications guide and Apple Platform Security guide 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

No non-administrator guidance.

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.

11.5 End of Life

The module secure sanitization is accomplished by first powering the module down, which will zeroize all SSPs within volatile memory. Following the power-down, an uninstall by way of system wipe or system update will zeroize the corecrypto-1638.100.62 binary file listed in Table 2.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.