Cryptographic Module Validation Program CMVP

Certificate #4392

Details

Module Name	Apple corecrypto Module v11.1 [Apple silicon, Kernel, Software]
Standard	FIPS 140-3
Status	Active
Sunset Date	12/6/2027
Overall Level	1
Caveat	When operated in approved mode
Security Level Exceptions	• Physical security: N/A • Non-invasive security: N/A • Mitigation of other attacks: N/A
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	The Apple corecrypto Kernel Space Module for Apple silicon is a software cryptographic module running on a multi-chip standalone hardware device and provides services intended to protect data in transit and at rest.
Tested Configuration(s)	• iOS 14.2 running on iPhone 11 Pro with an Apple A Series A13 Bionic with PAA • iOS 14.2 running on iPhone 11 Pro with an Apple A Series A13 Bionic without PAA • iOS 14.2 running on iPhone 12 with an Apple A Series A14 Bionic with PAA • iOS 14.2 running on iPhone 12 with an Apple A Series A14 Bionic without PAA • iOS 14.2 running on iPhone 6S with an Apple A Series A9 with PAA • iOS 14.2 running on iPhone 6S with an Apple A Series A9 without PAA • iOS 14.2 running on iPhone 7 Plus with an Apple A Series A10 Fusion with PAA • iOS 14.2 running on iPhone 7 Plus with an Apple A Series A10 Fusion without PAA • iOS 14.2 running on iPhone X with an Apple A Series A11 Bionic with PAA • iOS 14.2 running on iPhone X with an Apple A Series A11 Bionic without PAA • iOS 14.2 running on iPhone XS Max with an Apple A Series A12 Bionic with PAA • iOS 14.2 running on iPhone XS Max with an Apple A Series A12 Bionic without PAA • iPadOS 14.2 running on iPad (5th generation) with an Apple A Series A9 with PAA • iPadOS 14.2 running on iPad (5th generation) with an Apple A Series A9 without PAA • iPadOS 14.2 running on iPad (7th generation) with an Apple A Series A10 Fusion with PAA • iPadOS 14.2 running on iPad (7th generation) with an Apple A Series A10 Fusion without PAA • iPadOS 14.2 running on iPad Air (4th generation) with an Apple A Series A14 Bionic with PAA • iPadOS 14.2 running on iPad Air (4th generation) with an Apple A Series A14 Bionic without PAA • iPadOS 14.2 running on iPad mini (5th generation) with an Apple A Series A12 Bionic with PAA • iPadOS 14.2 running on iPad mini (5th generation) with an Apple A Series A12 Bionic without PAA • iPadOS 14.2 running on iPad Pro 10.5 inch with an Apple A Series A10X Fusion with PAA • iPadOS 14.2 running on iPad Pro 10.5 inch with an Apple A Series A10X Fusion without PAA • iPadOS 14.2 running on iPad Pro 11in (2nd generation) with an Apple A Series A12Z Bionic with PAA • iPadOS 14.2 running on iPad Pro 11in (2nd generation) with an Apple A Series A12Z Bionic without PAA • iPadOS 14.2 running on iPad Pro 11-inch (1st generation) with an Apple A Series A12X Bionic with PAA • iPadOS 14.2 running on iPad Pro 11-inch (1st generation) with an Apple A Series A12X Bionic without PAA • iPadOS 14.2 running on iPad Pro 9.7-inch with an Apple A Series A9X with PAA • iPadOS 14.2 running on iPad Pro 9.7-inch with an Apple A Series A9X without PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Apple M Series M1 with PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Apple M Series M1 without PAA • tvOS 14.2 running on Apple TV 4K with an Apple A Series A10X Fusion with PAA • tvOS 14.2 running on Apple TV 4K with an Apple A Series A10X Fusion without PAA • TxFW 11.0.1 running on Apple Security Chip T2 with an Apple T Series T2 with PAA • TxFW 11.0.1 running on Apple Security Chip T2 with an Apple T Series T2 without PAA • watchOS 7.1 running on Apple Watch Series S3 with an Apple S Series S3 with PAA • watchOS 7.1 running on Apple Watch Series S3 with an Apple S Series S3 without PAA • watchOS 7.1 running on Apple Watch Series S4 with an Apple S Series S4 with PAA • watchOS 7.1 running on Apple Watch Series S4 with an Apple S Series S4 without PAA • watchOS 7.1 running on Apple Watch Series S5 with an Apple S Series S5 with PAA • watchOS 7.1 running on Apple Watch Series S5 with an Apple S Series S5 without PAA • watchOS 7.1 running on Apple Watch Series S6 with an Apple S Series S6 with PAA • watchOS 7.1 running on Apple Watch Series S6 with an Apple S Series S6 without PAA

Approved Algorithms	
AES-CBC	A945
AES-CBC	A946
AES-CCM	A943
AES-CFB128	A945
AES-CFB128	A946
AES-CFB8	A945
AES-CTR	A943
AES-CTR	A945
AES-ECB	A943
AES-ECB	A945
AES-ECB	A946
AES-GCM	A943
AES-KW	A945
AES-OFB	A945
AES-OFB	A946
AES-XTS	A946
Counter DRBG	A943
Counter DRBG	A945
ECDSA KeyGen (FIPS186-4)	A942
ECDSA KeyVer (FIPS186-4)	A942
ECDSA SigGen (FIPS186-4)	A942
ECDSA SigVer (FIPS186-4)	A942
HMAC DRBG	A942
HMAC DRBG	A944
HMAC-SHA-1	A942
HMAC-SHA2-224	A942
HMAC-SHA2-256	A942
HMAC-SHA2-256	A947
HMAC-SHA2-384	A942
HMAC-SHA2-384	A944
HMAC-SHA2-512	A942
HMAC-SHA2-512	A944
HMAC-SHA2-512/256	A942
HMAC-SHA2-512/256	A944
RSA SigGen (FIPS186-4)	A942
RSA SigVer (FIPS186-4)	A942
SHA-1	A942
SHA2-224	A942
SHA2-256	A942
SHA2-256	A947
SHA2-384	A942
SHA2-384	A944
SHA2-512	A944
SHA2-512/256	A942
SHA2-512/256	A944

Entropy	ENT (P), ENT (NP)
Software Versions	11.1
Product URL	https://support.apple.com/guide/certifications/welcome/web

Vendor

Apple Inc.
One Apple Park Way
MS: 927-1CPS
Cupertino, CA 95014
USA

Shawn Geddis
security-certifications@apple.com
Phone: 6692273579
Fax: 866-315-1954

Fiona Pattinson
security-certifications@apple.com
Phone: 737-219-4141

Related Files

Security Policy
Consolidated Certificate

Validation History

Date	Type	Lab
12/7/2022	Initial	ATSEC INFORMATION SECURITY CORP