An official website of the United States government Here's how you know

Cryptographic Module Validation Program CMVP

Certificate #4391

Details

Module Name	Apple corecrypto Module v11.1 [Apple silicon, User, 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 User 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 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 11-inch (2nd generation) with an Apple A Series A12Z Bionic with PAA • iPadOS 14.2 running on iPad Pro 11-inch (2nd generation) with an Apple A Series A12Z 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	A916
AES-CBC	A919
AES-CBC	A920
AES-CBC	A921
AES-CCM	A918
AES-CCM	A919
AES-CCM	A921
AES-CFB128	A916
AES-CFB128	A919
AES-CFB128	A921
AES-CFB8	A919
AES-CFB8	A921
AES-CMAC	A919
AES-CTR	A918
AES-CTR	A919
AES-CTR	A921
AES-ECB	A916
AES-ECB	A918
AES-ECB	A919
AES-ECB	A921
AES-GCM	A918
AES-GCM	A919
AES-GCM	A921
AES-KW	A919
AES-KW	A921
AES-OFB	A916
AES-OFB	A919
AES-OFB	A921
AES-XTS	A916
AES-XTS	A919
AES-XTS	A921
Counter DRBG	A918
Counter DRBG	A919
Counter DRBG	A921
ECDSA KeyGen (FIPS186-4)	A917
ECDSA KeyGen (FIPS186-4)	A919
ECDSA KeyVer (FIPS186-4)	A917
ECDSA KeyVer (FIPS186-4)	A919
ECDSA SigGen (FIPS186-4)	A917
ECDSA SigGen (FIPS186-4)	A919
ECDSA SigVer (FIPS186-4)	A917
ECDSA SigVer (FIPS186-4)	A919
HMAC DRBG	A917
HMAC DRBG	A919
HMAC-SHA-1	A917
HMAC-SHA-1	A919
HMAC-SHA2-224	A917
HMAC-SHA2-224	A919
HMAC-SHA2-256	A917
HMAC-SHA2-256	A919
HMAC-SHA2-256	A922
HMAC-SHA2-384	A917
HMAC-SHA2-384	A919
HMAC-SHA2-512	A917
HMAC-SHA2-512	A919
HMAC-SHA2-512/256	A917
HMAC-SHA2-512/256	A919
KAS-ECC-SSC Sp800-56Ar3	A919
KAS-FFC-SSC Sp800-56Ar3	A919
KDF SP800-108	A917
KDF SP800-108	A919
PBKDF	A917
PBKDF	A919
RSA KeyGen (FIPS186-4)	A917
RSA KeyGen (FIPS186-4)	A919
RSA SigGen (FIPS186-4)	A917
RSA SigGen (FIPS186-4)	A919
RSA SigVer (FIPS186-4)	A917
RSA SigVer (FIPS186-4)	A919
Safe Primes Key Generation	A919
SHA-1	A917
SHA-1	A919
SHA2-224	A917
SHA2-224	A919
SHA2-256	A917
SHA2-256	A919
SHA2-256	A922
SHA2-384	A917
SHA2-384	A919
SHA2-512	A917
SHA2-512	A919
SHA2-512/256	A917
SHA2-512/256	A919

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 Stewart
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