Cryptographic Module Validation Program CMVP

Certificate #3856

Details

Module Name	Apple corecrypto User Space Module for ARM (ccv10)
Standard	FIPS 140-2
Status	Active
Sunset Date	3/22/2026
Validation Dates	03/23/2021
Overall Level	1
Caveat	When operated in FIPS Mode
Security Level Exceptions	• Physical Security: N/A
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	The Apple corecrypto User Space Module for ARM (ccv10) 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 13 running on iPhone 11 Pro Max with Apple A13 Bionic with PAA
- iOS 13 running on iPhone 11 Pro Max with Apple A13 Bionic without PAA
- iOS 13 running on iPhone 6S Plus with Apple A9 with PAA
- iOS 13 running on iPhone 6S Plus with Apple A9 without PAA
- iOS 13 running on iPhone 7 Plus with Apple A10 Fusion with PAA
- iOS 13 running on iPhone 7 Plus with Apple A10 Fusion without PAA
- iOS 13 running on iPhone 8 Plus with Apple A11 Bionic with PAA
- iOS 13 running on iPhone 8 Plus with Apple A11 Bionic without PAA
- iOS 13 running on iPhone Xs Max with Apple A12 Bionic with PAA
- iOS 13 running on iPhone Xs Max with Apple A12 Bionic without PAA
- iPadOS 13 running on iPad (5th generation) with Apple A9 with PAA
- iPadOS 13 running on iPad (5th generation) with Apple A9 without PAA
- iPadOS 13 running on iPad (6th generation) with Apple A10 Fusion with PAA
- iPadOS 13 running on iPad (6th generation) with Apple A10 Fusion without PAA
- iPadOS 13 running on iPad Air 2 with Apple A8X with PAA
- iPadOS 13 running on iPad Air 2 with Apple A8X without PAA
- iPadOS 13 running on iPad mini (5th generation) with Apple A12 Bionic with PAA
- iPadOS 13 running on iPad mini (5th generation) with Apple A12 Bionic without PAA
- iPadOS 13 running on iPad mini 4 with Apple A8 with PAA
- iPadOS 13 running on iPad mini 4 with Apple A8 without PAA
- iPadOS 13 running on iPad Pro (12.9 inch, 2nd generation) with Apple A10X Fusion with PAA
- iPadOS 13 running on iPad Pro (12.9 inch, 2nd generation) with Apple A10X Fusion without PAA
- iPadOS 13 running on iPad Pro (12.9 inch, 3rd generation) with Apple A12X Bionic with PAA
- iPadOS 13 running on iPad Pro (12.9 inch, 3rd generation) with Apple A12X Bionic without PAA
- iPadOS 13 running on iPad Pro (9.7 inch) with Apple A9X with PAA
- iPadOS 13 running on iPad Pro (9.7 inch) with Apple A9X without PAA
- tvOS 13 running on Apple TV 4K with Apple A10X Fusion with PAA
- tvOS 13 running on Apple TV 4K with Apple A10X Fusion without PAA
- TxFW 10.15 running on Apple T2 with PAA
- TxFW 10.15 running on Apple T2 without PAA (single-user mode)
- watchOS 6 running on Apple Watch Series 1 with Apple S1P with PAA
- watchOS 6 running on Apple Watch Series 1 with Apple S1P without PAA
- watchOS 6 running on Apple Watch Series 3 with Apple S3 with PAA
- watchOS 6 running on Apple Watch Series 3 with Apple S3 without PAA
- watchOS 6 running on Apple Watch Series 4 with Apple S4 with PAA
- watchOS 6 running on Apple Watch Series 4 with Apple S4 without PAA
- watchOS 6 running on Apple Watch Series 5 with Apple S5 with PAA
- watchOS 6 running on Apple Watch Series 5 with Apple S5 without PAA

FIPS Algorithms

AES	Certs. #A6, #A7, #A8, #A10 and #A11
CVL	Cert. #A8
DRBG	Certs. #A7, #A8, #A9 and #A10
ECDSA	Certs. #A8 and #A9
HMAC	Certs. #A8, #A9 and #A12
KTS	AES Certs. #A7, #A8 and #A10; key establishment methodology provides between 128 and 256 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed
RSA	Certs. #A8 and #A9
SHS	Certs. #A8, #A9 and #A12
Triple-DES	Cert. #A8

Allowed Algorithms	Diffie-Hellman (CVL Cert. #A8, key agreement; key establishment methodology provides 112 bits of encryption strength); EC Diffie-Hellman (CVL Cert. #A8, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength); MD5; NDRNG; RSA (key wrapping; key establishment methodology provides between 112 and 152 bits of encryption strength)
Software Versions	10.0
Product URL	http://www.support.apple.com/guide/sccc/welcome/web

Vendor

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

Shawn Geddis
security-certifications@apple.com
Phone: 669-227-3579

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

Related Files

Security Policy

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0

NIST National Institute of Standards and Technology U.S. Department of Commerce

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications? Subscribe

Webmaster | Contact Us | Our Other Offices

Contact CSRC Webmaster: webmaster-csrc@nist.gov

Privacy Statement | Privacy Policy | Security Notice | Accessibility Statement | NIST Privacy Program | No Fear Act Policy | Disclaimer | FOIA | Environmental Policy Statement

Cookie Disclaimer | Scientific Integrity Summary | NIST Information Quality Standards | Commerce.gov | Healthcare.gov | Science.gov | USA.gov