# Cryptographic Module Validation Program CMVP

## Certificate #3855

### Details

| | |
|---|---|
| Module Name | Apple corecrypto Kernel 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 Kernel 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<br>• iOS 13 running on iPhone 11 Pro Max with Apple A13 Bionic without PAA<br>• iOS 13 running on iPhone 6S Plus with Apple A9 with PAA<br>• iOS 13 running on iPhone 6S Plus with Apple A9 without PAA<br>• iOS 13 running on iPhone 7 Plus with Apple A10 Fusion with PAA<br>• iOS 13 running on iPhone 7 Plus with Apple A10 Fusion without PAA<br>• iOS 13 running on iPhone 8 Plus with Apple A11 Bionic with PAA<br>• iOS 13 running on iPhone 8 Plus with Apple A11 Bionic without PAA<br>• iOS 13 running on iPhone Xs Max with Apple A12 Bionic with PAA<br>• iOS 13 running on iPhone Xs Max with Apple A12 Bionic without PAA<br>• iPadOS 13 running on iPad (5th generation) with Apple A9 with PAA<br>• iPadOS 13 running on iPad (5th generation) with Apple A9 without PAA<br>• iPadOS 13 running on iPad (6th generation) with Apple A10 Fusion with PAA<br>• iPadOS 13 running on iPad (6th generation) with Apple A10 Fusion without PAA<br>• iPadOS 13 running on iPad Air 2 with Apple A8X with PAA<br>• iPadOS 13 running on iPad Air 2 with Apple A8X without PAA<br>• iPadOS 13 running on iPad mini (5th generation) with Apple A12 Bionic with PAA<br>• iPadOS 13 running on iPad mini (5th generation) with Apple A12 Bionic without PAA<br>• iPadOS 13 running on iPad mini 4 with Apple A8 with PAA<br>• iPadOS 13 running on iPad mini 4 with Apple A8 without PAA<br>• iPadOS 13 running on iPad Pro (12.9 inch, 2nd generation) with Apple A10X Fusion with PAA<br>• iPadOS 13 running on iPad Pro (12.9 inch, 2nd generation) with Apple A10X Fusion without PAA<br>• iPadOS 13 running on iPad Pro (12.9 inch, 3rd generation) with Apple A12X Bionic with PAA<br>• iPadOS 13 running on iPad Pro (12.9 inch, 3rd generation) with Apple A12X Bionic without PAA<br>• iPadOS 13 running on iPad Pro (9.7 inch) with Apple A9X with PAA<br>• iPadOS 13 running on iPad Pro (9.7 inch) with Apple A9X without PAA<br>• tvOS 13 running on Apple TV 4K with Apple A10X Fusion with PAA<br>• tvOS 13 running on Apple TV 4K with Apple A10X Fusion without PAA<br>• TxFW 10.15 running on Apple T2 with PAA<br>• TxFW 10.15 running on Apple T2 without PAA (single-user mode)<br>• watchOS 6 running on Apple Watch Series 1 with Apple S1P with PAA<br>• watchOS 6 running on Apple Watch Series 1 with Apple S1P without PAA<br>• watchOS 6 running on Apple Watch Series 3 with Apple S3 with PAA<br>• watchOS 6 running on Apple Watch Series 3 with Apple S3 without PAA<br>• watchOS 6 running on Apple Watch Series 4 with Apple S4 with PAA<br>• watchOS 6 running on Apple Watch Series 4 with Apple S4 without PAA<br>• watchOS 6 running on Apple Watch Series 5 with Apple S5 with PAA<br>• watchOS 6 running on Apple Watch Series 5 with Apple S5 without PAA |
| FIPS Algorithms | AES: Certs. #A13, #A14 and #A15<br>DRBG: Certs. #A13, #A15, #A16 and #A18<br>ECDSA: Cert. #A18<br>HMAC: Certs. #A16, #A17 and #A18<br>KTS: AES Certs. #A13 and #A15; key establishment methodology provides between 128 and 256 bits of encryption strength<br>RSA: Cert. #A18<br>SHS: Certs. #A16, #A17 and #A18<br>Triple-DES: Cert. #A16 |
| Allowed Algorithms | 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