Cryptographic Module Validation Program CMVP

Certificate #3858

Details

Module Name	Apple corecrypto Kernel Space Module for Intel (ccv10)
Standard	FIPS 140-2
Status	Active
Sunset Date	3/23/2026
Validation Dates	03/24/2021
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 Intel (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)	• macOS Catalina 10.15 running on iMac Pro with Intel Xeon W with PAA • macOS Catalina 10.15 running on iMac Pro with Intel Xeon W without PAA • macOS Catalina 10.15 running on Mac mini with Intel Core i5 with PAA • macOS Catalina 10.15 running on Mac mini with Intel Core i5 without PAA • macOS Catalina 10.15 running on MacBook Pro with Intel Core i7 with PAA • macOS Catalina 10.15 running on MacBook Pro with Intel Core i7 without PAA • macOS Catalina 10.15 running on MacBook Pro with Intel Core i9 with PAA • macOS Catalina 10.15 running on MacBook Pro with Intel Core i9 without PAA • macOS Catalina 10.15 running on MacBook with Intel Core M with PAA • macOS Catalina 10.15 running on MacBook with Intel Core M without PAA (single-user mode)

FIPS Algorithms

AES	Certs. #A13, #A15, #A20, #A23, #A24 and #A28
DRBG	Certs. #A13, #A15, #A23, #A26, #A28, #A30 and #A34
ECDSA	Certs. #A26, #A30 and #A34
HMAC	Certs. #A26, #A30, #A32 and #A34
KTS	AES Certs. #A13, #A15, #A23 and #A28; key establishment methodology provides between 128 and 256 bits of encryption strength
PBKDF	vendor affirmed
RSA	Certs. #A26, #A30 and #A34
SHS	Certs. #A26, #A30, #A32 and #A34
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
Consolidated Certificate

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0