Cryptographic Module Validation Program CMVP

Certificate #3859

Details

Module Name	Apple corecrypto User 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 User 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 an Intel Xeon W with PAA • macOS Catalina 10.15 running on iMac Pro with an Intel Xeon W without PAA • macOS Catalina 10.15 running on Mac mini with an Intel Core i5 with PAA • macOS Catalina 10.15 running on Mac mini with an Intel Core i5 without PAA • macOS Catalina 10.15 running on MacBook Pro with an Intel Core i7 with PAA • macOS Catalina 10.15 running on MacBook Pro with an Intel Core i7 without PAA • macOS Catalina 10.15 running on MacBook Pro with an Intel Core i9 with PAA • macOS Catalina 10.15 running on MacBook Pro with an Intel Core i9 without PAA • macOS Catalina 10.15 running on MacBook with an Intel Core M with PAA • macOS Catalina 10.15 running on MacBook with an Intel Core M without PAA (single-user mode)

FIPS Algorithms

AES	Certs. #A7, #A8, #A10, #A11, #A19, #A21, #A25 and #A31
CVL	Cert. #A8
DRBG	Certs. #A7, #A8, #A10, #A21, #A22, #A27, #A31 and #A33
ECDSA	Certs. #A8, #A22, #A27 and #A33
HMAC	Certs. #A8, #A22, #A27, #A29 and #A33
KTS	AES Certs. #A7, #A8, #A10, #A21 and #A31; key establishment methodology provides between 128 and 256 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed
RSA	Certs. #A8, #A22, #A27 and #A33
SHS	Certs. #A8, #A22, #A27, #A29 and #A33
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
Consolidated Certificate

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0