Cryptographic Module Validation Program CMVP

Certificate #4389

Details

Module Name	Apple corecrypto Module v11.1 [Intel, 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 Intel 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 Big Sur 11.0.1 running on iMac Pro with a Xeon W-2140B (Sky Lake) with PAA • macOS Big Sur 11.0.1 running on iMac Pro with a Xeon W-2140B (Sky Lake) without PAA • macOS Big Sur 11.0.1 running on Mac Pro with a Xeon W-3223 (Cascade Lake) with PAA • macOS Big Sur 11.0.1 running on Mac Pro with a Xeon W-3223 (Cascade Lake) without PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Intel i5-8210Y (Amber Lake) with PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Intel i5-8210Y (Amber Lake) without PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Intel i7-1060NG7 (Ice Lake) with PAA • macOS Big Sur 11.0.1 running on MacBook Air with an Intel i7-1060NG7 (Ice Lake) without PAA • macOS Big Sur 11.0.1 running on MacBook Pro with an Intel i7-8850H (Coffee Lake) with PAA • macOS Big Sur 11.0.1 running on MacBook Pro with an Intel i7-8850H (Coffee Lake) without PAA • macOS Big Sur 11.0.1 running on MacBook Pro with an Intel i9-9880H (Coffee Lake) with PAA • macOS Big Sur 11.0.1 running on MacBook Pro with an Intel i9-9880H (Coffee Lake) without PAA

Approved Algorithms	
AES-CBC	A919
AES-CBC	A920
AES-CBC	A921
AES-CBC	A925
AES-CBC	A926
AES-CBC	A927
AES-CCM	A918
AES-CCM	A919
AES-CCM	A921
AES-CCM	A925
AES-CCM	A929
AES-CFB128	A919
AES-CFB128	A921
AES-CFB128	A925
AES-CFB8	A919
AES-CFB8	A921
AES-CFB8	A925
AES-CMAC	A919
AES-CTR	A918
AES-CTR	A919
AES-CTR	A921
AES-CTR	A925
AES-CTR	A929
AES-ECB	A918
AES-ECB	A919
AES-ECB	A921
AES-ECB	A925
AES-ECB	A926
AES-ECB	A927
AES-ECB	A929
AES-GCM	A918
AES-GCM	A919
AES-GCM	A921
AES-GCM	A925
AES-GCM	A929
AES-KW	A919
AES-KW	A921
AES-KW	A925
AES-OFB	A919
AES-OFB	A921
AES-OFB	A925
AES-XTS	A919
AES-XTS	A921
AES-XTS	A925
AES-XTS	A926
AES-XTS	A927
Counter DRBG	A918
Counter DRBG	A919
Counter DRBG	A921
Counter DRBG	A925
Counter DRBG	A929
ECDSA KeyGen (FIPS186-4)	A919
ECDSA KeyGen (FIPS186-4)	A923
ECDSA KeyGen (FIPS186-4)	A924
ECDSA KeyGen (FIPS186-4)	A930
ECDSA KeyVer (FIPS186-4)	A919
ECDSA KeyVer (FIPS186-4)	A923
ECDSA KeyVer (FIPS186-4)	A924
ECDSA KeyVer (FIPS186-4)	A930
ECDSA SigGen (FIPS186-4)	A919
ECDSA SigGen (FIPS186-4)	A923
ECDSA SigGen (FIPS186-4)	A924
ECDSA SigGen (FIPS186-4)	A930
ECDSA SigVer (FIPS186-4)	A919
ECDSA SigVer (FIPS186-4)	A923
ECDSA SigVer (FIPS186-4)	A924
ECDSA SigVer (FIPS186-4)	A930
HMAC DRBG	A919
HMAC DRBG	A923
HMAC DRBG	A924
HMAC DRBG	A930
HMAC-SHA-1	A919
HMAC-SHA-1	A923
HMAC-SHA-1	A924
HMAC-SHA-1	A928
HMAC-SHA-1	A930
HMAC-SHA2-224	A919
HMAC-SHA2-224	A923
HMAC-SHA2-224	A924
HMAC-SHA2-224	A928
HMAC-SHA2-224	A930
HMAC-SHA2-256	A919
HMAC-SHA2-256	A923
HMAC-SHA2-256	A924
HMAC-SHA2-256	A928
HMAC-SHA2-256	A930
HMAC-SHA2-384	A919
HMAC-SHA2-384	A923
HMAC-SHA2-384	A924
HMAC-SHA2-384	A928
HMAC-SHA2-384	A930
HMAC-SHA2-512	A919
HMAC-SHA2-512	A923
HMAC-SHA2-512	A924
HMAC-SHA2-512	A928
HMAC-SHA2-512	A930
HMAC-SHA2-512/256	A919
HMAC-SHA2-512/256	A923
HMAC-SHA2-512/256	A924
HMAC-SHA2-512/256	A930
KAS-ECC-SSC Sp800-56Ar3	A919
KAS-FFC-SSC Sp800-56Ar3	A919
KDF SP800-108	A919
KDF SP800-108	A919
KDF SP800-108	A923
KDF SP800-108	A924
KDF SP800-108	A930
PBKDF	A919
PBKDF	A923
PBKDF	A924
PBKDF	A930
RSA KeyGen (FIPS186-4)	A919
RSA KeyGen (FIPS186-4)	A923
RSA KeyGen (FIPS186-4)	A924
RSA KeyGen (FIPS186-4)	A930
RSA SigGen (FIPS186-4)	A919
RSA SigGen (FIPS186-4)	A923
RSA SigGen (FIPS186-4)	A924
RSA SigGen (FIPS186-4)	A930
RSA SigVer (FIPS186-4)	A919
RSA SigVer (FIPS186-4)	A923
RSA SigVer (FIPS186-4)	A924
RSA SigVer (FIPS186-4)	A930
Safe-Primes Key Generation	A919
SHA-1	A919
SHA-1	A923
SHA-1	A924
SHA-1	A928
SHA-1	A930
SHA2-224	A919
SHA2-224	A923
SHA2-224	A924
SHA2-224	A928
SHA2-224	A930
SHA2-256	A919
SHA2-256	A923
SHA2-256	A924
SHA2-256	A928
SHA2-256	A930
SHA2-384	A919
SHA2-384	A923
SHA2-384	A924
SHA2-384	A928
SHA2-384	A930
SHA2-512	A919
SHA2-512	A923
SHA2-512	A924
SHA2-512	A928
SHA2-512	A930
SHA2-512/256	A919
SHA2-512/256	A923
SHA2-512/256	A924
SHA2-512/256	A930
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-certification@apple.com
Phone: 669-227-3579
Fax: 866-315-1954
Fiona Stewart
security-certification@apple.com
Phone: 512-825-3083

Related Files

Security Policy
Consolidated Certificate

Validation History

Date	Type	Lab
12/7/2022	Initial	ATSEC INFORMATION SECURITY CORP