Cryptographic Module Validation Program CMVP

Certificate #4390

Details

Module Name	Apple corecrypto Module v11.1 [Intel, Kernel, 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 Kernel 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	A945
AES-CBC	A976
AES-CBC	A977
AES-CBC	A978
AES-CCM	A943
AES-CCM	A973
AES-CFB128	A945
AES-CFB128	A976
AES-CFB8	A945
AES-CFB8	A976
AES-CTR	A943
AES-CTR	A945
AES-CTR	A973
AES-CTR	A976
AES-ECB	A943
AES-ECB	A945
AES-ECB	A973
AES-ECB	A976
AES-ECB	A977
AES-ECB	A978
AES-GCM	A943
AES-GCM	A973
AES-KW	A945
AES-KW	A976
AES-OFB	A945
AES-OFB	A976
AES-XTS	A977
AES-XTS	A978
Counter DRBG	A943
Counter DRBG	A945
Counter DRBG	A973
Counter DRBG	A976
ECDSA KeyGen (FIPS186-4)	A974
ECDSA KeyGen (FIPS186-4)	A975
ECDSA KeyGen (FIPS186-4)	A990
ECDSA KeyVer (FIPS186-4)	A974
ECDSA KeyVer (FIPS186-4)	A975
ECDSA KeyVer (FIPS186-4)	A990
ECDSA SigGen (FIPS186-4)	A974
ECDSA SigGen (FIPS186-4)	A975
ECDSA SigGen (FIPS186-4)	A990
ECDSA SigVer (FIPS186-4)	A974
ECDSA SigVer (FIPS186-4)	A975
ECDSA SigVer (FIPS186-4)	A990
HMAC DRBG	A974
HMAC DRBG	A975
HMAC DRBG	A990
HMAC-SHA-1	A974
HMAC-SHA-1	A975
HMAC-SHA-1	A979
HMAC-SHA-1	A990
HMAC-SHA2-224	A974
HMAC-SHA2-224	A975
HMAC-SHA2-224	A979
HMAC-SHA2-224	A990
HMAC-SHA2-256	A974
HMAC-SHA2-256	A975
HMAC-SHA2-256	A979
HMAC-SHA2-256	A990
HMAC-SHA2-384	A974
HMAC-SHA2-384	A975
HMAC-SHA2-384	A979
HMAC-SHA2-384	A990
HMAC-SHA2-512	A974
HMAC-SHA2-512	A975
HMAC-SHA2-512	A979
HMAC-SHA2-512	A990
HMAC-SHA2-512/256	A974
HMAC-SHA2-512/256	A975
HMAC-SHA2-512/256	A990
KDF SP800-108	A990
RSA KeyGen (FIPS186-4)	A974
RSA KeyGen (FIPS186-4)	A975
RSA KeyGen (FIPS186-4)	A990
RSA SigGen (FIPS186-4)	A974
RSA SigGen (FIPS186-4)	A975
RSA SigGen (FIPS186-4)	A990
RSA SigVer (FIPS186-4)	A974
RSA SigVer (FIPS186-4)	A975
RSA SigVer (FIPS186-4)	A990
SHA-1	A974
SHA-1	A975
SHA-1	A979
SHA-1	A990
SHA2-224	A974
SHA2-224	A975
SHA2-224	A979
SHA2-224	A990
SHA2-256	A974
SHA2-256	A975
SHA2-256	A979
SHA2-256	A990
SHA2-384	A974
SHA2-384	A975
SHA2-384	A979
SHA2-384	A990
SHA2-512	A974
SHA2-512	A975
SHA2-512	A979
SHA2-512	A990
SHA2-512/256	A974
SHA2-512/256	A975
SHA2-512/256	A990

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
geddis@apple.com
Phone: 6692273579
Fax: 866-315-1954

Fiona Stewart
f_stewart@apple.com
Phone: 5128253083

Related Files

Security Policy
Consolidated Certificate

Validation History

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