Cryptographic Module Validation Program

Certificate #3156

Details

Module Name	Apple CoreCrypto Kernel Module v8.0 for Intel
Standard	FIPS 140-2
Status	Active
Sunset Date	3/21/2023
Validation Dates	3/22/2018
Overall Level	1
Caveat	When operated in FIPS mode. The module generates cryptographic keys whose strengths are modified by available entropy
Security Level Exceptions	• Physical Security: N/A
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	The Apple CoreCrypto Kerenl Module v8.0 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 High Sierra 10.13 running on iMac Pro with Xeon CPU with PAA • macOS High Sierra 10.13 running on iMac Pro with Xeon CPU without PAA • macOS High Sierra 10.13 running on Mac mini with i5 CPU with PAA • macOS High Sierra 10.13 running on Mac mini with i5 CPU without PAA • macOS High Sierra 10.13 running on MacBook Pro with i7 CPU with PAA • macOS High Sierra 10.13 running on MacBook Pro with i7 CPU without PAA • macOS High Sierra 10.13 running on MacBook with Core M CPU with PAA • macOS High Sierra 10.13 running on MacBook with Core M CPU without PAA (single-user mode)

FIPS Algorithms

AES	Certs. #4985, #4986, #4987, #4988, #4989, #4990, #4991, #4992, #4993, #4994, #4995, #4996, #5054, #5055, #5056, #5057, #5063, #5065, #5071 and #5072
DRBG	Certs. #1804, #1805, #1806, #1807, #1808, #1809, #1810, #1811, #1812, #1813, #1814, #1815, #1816, #1817, #1818, #1819, #1872, #1873, #1874, #1875, #1876, #1877, #1878, #1882, #1883, #1885, #1888 and #1889
ECDSA	Certs. #1308, #1309, #1310 and #1313
HMAC	Certs. #3308, 3309, 3310, #3311, #3312, #3313, #3314, #3315, #3316, #3317, #3318, #3319, #3375, #3376, #3377 and #3382
KTS	AES Certs. #4985, #4986, #4987, #4988, #4989, #4990, #4991, #4992, #4993, #4994, #4995, #4996, #5054, #5055, #5056, #5057, #5063, #5065, #5071 and #5072; key establishment methodology provides 128 or 160 bits of encryption strength
PBKDF	vendor affirmed
RSA	Certs. #2740, #2741, #2742 and #2748
SHS	Certs. #4051, #4052, #4053, #4054, #4055, #4056, #4057, #4058, #4059, #4060, #4061, #4062, #4120, #4121, #4122 and #4127
Triple-DES	Certs. #2613, #2614, #2615 and #2618

Allowed Algorithms	MD5; NDRNG; RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
Software Versions	8.0
Product URL	http://support.apple.com/en-us/HT202739

Vendor

Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
USA

Shawn Geddis
geddis@apple.com
Phone: 669-227-3579
Fax: 866-315-1954

Related Files

Security Policy
Consolidated Certificate

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0