Cryptographic Module Validation Program

Certificate #3155

Details

Module Name	Apple CoreCrypto 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 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 v10.13 running on iMac Pro with Xeon CPU with PAA • macOS High Sierra v10.13 running on iMac Pro with Xeon CPU without PAA • macOS High Sierra v10.13 running on Mac mini with i5 CPU with PAA • macOS High Sierra v10.13 running on Mac mini with i5 CPU without PAA • macOS High Sierra v10.13 running on MacBook Pro with i7 CPU with PAA • macOS High Sierra v10.13 running on MacBook Pro with i7 CPU without PAA • macOS High Sierra v10.13 running on MacBook with Core M CPU with PAA • macOS High Sierra v10.13 running on MacBook with Core M CPU without PAA (single-user mode)

FIPS Algorithms

AES	Certs. #4944, #4945, #4946, #4947, #4948, #4949, #4950, #4951, #4952, #4953, #4954, #4955, #4961, #4962, #4963, #4964, #4965, #4966, #4967, #4968, #4969, #4970, #4971, #4972, #4973, #4974, #4975, #4976, #5048, #5049, #5050 and #5051
CVL	Certs. #1602, #1603, #1604, #1605, #1606, #1607, #1608 and #1609
DRBG	Certs. #1771, #1772, #1773, #1774, #1775, #1776, #1777, #1778, #1779, #1780, #1781, #1782, #1783, #1784, #1785, #1786, #1789, #1790, #1791, #1792, #1793, #1794, #1795, #1796, #1868, #1869, #1870 and #1871
ECDSA	Certs. #1304, #1305, #1306 and #1307
HMAC	Certs. #3292, #3293, #3294, #3295, #3296, #3297, #3298, #3299, #3300, #3301, #3302, #3303, #3371, #3372, #3373 and #3374
KTS	AES Certs. #4944, #4945, #4946, #4947, #4948, #4949, #4950, #4951, #4961, #4962, #4963, #4964, #4965, #4966, #4967, #4968, #4969, #4970, #4971, #4972, #4973, #4974, #4975, #4976, #5048, #5049, #5050 and #5051; key establishment methodology provides between 128 or 160 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed
RSA	Certs. #2734, #2735, #2736 and #2737
SHS	Certs. #4034, #4035, #4036, #4037, #4038, #4039, #4040, #4041, #4042, #4043, #4044, #4045, #4116, #4117, #4118 and #4119
Triple-DES	Certs. #2609, #2610, #2611 and #2612

Allowed Algorithms	Diffie-Hellman (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 160 bits of encryption strength); 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/HT201159

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