Cryptographic Module Validation Program

Certificate #3402

Details

Module Name	Apple CoreCrypto Module v9.0 for Intel
Standard	FIPS 140-2
Status	Active
Sunset Date	3/12/2024
Validation Dates	3/13/2019 4/12/2019
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 Module v9.0 for Intel is a software cryptographic module running on a multi-chip standalo provides services intended to protect data in transit and at rest.
Tested Configuration(s)	• macOS Mojave 10.14 running on iMac Pro with Xeon CPU with PAA • macOS Mojave 10.14 running on iMac Pro with Xeon CPU without PAA • macOS Mojave 10.14 running on Mac mini with i5 CPU with PAA • macOS Mojave 10.14 running on Mac mini with i5 CPU without PAA • macOS Mojave 10.14 running on MacBook Pro with i7 CPU with PAA • macOS Mojave 10.14 running on MacBook Pro with i7 CPU without PAA • macOS Mojave 10.14 running on MacBook Pro with i9 CPU with PAA • macOS Mojave 10.14 running on MacBook Pro with i9 CPU without PAA • macOS Mojave 10.14 running on MacBook with Core M CPU with PAA • macOS Mojave 10.14 running on MacBook with Core M CPU without PAA (single-user mode)

FIPS Algorithms

AES	Certs. #5769, #5770, #5771, #5772, #5773, #5774, #5775, #5776, #5777, #5778, #5779, #5780, #5781, # #5785, #5786, #5787, #5788, #5789, #5790, #5791, #5792, #5793, #5800, #5801, #5802, #5803, #5804, #5808, #5809, #5810, #5811, #5812, #5813 and #5814
CVL	Certs. #2092, #2093, #2095, #2096, #2097, #2105, #2106, #2107, #2108 and #2109
DRBG	Certs. #2364, #2365, #2366, #2367, #2368, #2369, #2370, #2371, #2372, #2373, #2374, #2375, #2376, # #2380, #2381, #2382, #2383, #2384, #2385, #2386, #2387, #2388, #2393, #2394, #2395, #2396, #2397, #2401 and #2402
DSA	Certs. #1468, #1469, #1470, #1471 and #1472
ECDSA	Certs. #1553, #1554, #1555, #1556 and #1557
HMAC	Certs. #3817, #3818, #3819, #3820, #3821, #3822, #3823, #3824, #3825, #3826, #3827, #3828, #3829, #

		#3836, #3837, #3838 and #3839
	KTS	AES Certs. #5769, #5770, #5771, #5772, #5773, #5779, #5780, #5781, #5782, #5783, #5800, #5801, #58 establishment methodology provides between 128 and 256 bits of encryption strength
	KTS	vendor affirmed
	PBKDF	vendor affirmed
	RSA	Certs. #3073, #3074, #3075, #3076 and #3077
	SHS	Certs. #4592, #4593, #4594, #4595, #4596, #4597, #4598, #4599, #4600, #4601, #4602, #4603, #4604, # #4611, #4612, #4613 and #4614
	Triple-DES	Certs. #2856, #2857, #2858, #2859 and #2860
Allowed Algorithms	Diffie-Hellman (CVL Certs. #2092, #2093, #2095, #2096 and #2097, key agreement; key establishment methodolo of encryption strength); EC Diffie-Hellman (CVL Certs. #2092, #2093, #2095, #2096 and #2097, key agreement; key methodology provides 128 or 256 bits of encryption strength); MD5; NDRNG; RSA (key wrapping; key establishme 112 or 128 bits of encryption strength)	
Software Versions	9.0	
Product URL	http://support.apple.com/en-us/HT201159	

Vendor

Apple Inc.
One Apple Park Way
MS: 927-1CPS
Cupertino, CA 95014
USA

Shawn Geddis
geddis@apple.com
Phone: 669-227-3579
Fax: 866-315-1954
Stephanie Motre Martin
smotre@apple.com
Phone: 408-750-6235
Fax: 866-315-1954

Related Files

Security Policy
Consolidated Certificate

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our pu

Webmaster | Contact Us | Our Other Offices

PROJECTS

PUBLICATIONS
Draft Pubs
Final Pubs
FIPS
Special Publications (SPs)
NISTIRs
ITL Bulletins
White Papers

TOPICS
Security & Privacy
Applications
Technologies
Sectors
Laws & Regulations
Activities & Products

NEWS & UPDATES

EVENTS

GLOSSARY

ABOUT CSRC
Computer Security Division
Applied Cybersecurity Division
Contact Us

Information T

Compu

Applied Cy

Contact CSRC Webmast

Journal Articles
Conference Papers
Books