Cryptographic Module Validation Program

Certificate #3147

Details

Module Name
Apple CoreCrypto Kernel Module v8.0 for ARM

Standard
FIPS 140-2

Status
Active

Sunset Date
3/8/2023

Validation Dates
3/9/2018
5/17/2018
7/3/2018

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 Kernel Module v8.0 for ARM 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)

- iBridgeOS (15P2064) running on Apple iMac Pro with Apple T2 (iBridge 2,1) with PAA
- iBridgeOS (15P2064) running on Apple iMac Pro with Apple T2 (iBridge 2,1) without PAA (single-user mode)
- iOS 11 running on iPad Air 2 with Apple A8X CPU with PAA
- iOS 11 running on iPad Air 2 with Apple A8X CPU without PAA
- iOS 11 running on iPad Pro with Apple A10X Fusion CPU with PAA
- iOS 11 running on iPad Pro with Apple A10X Fusion CPU without PAA
- iOS 11 running on iPad Pro with Apple A9X CPU with PAA
- iOS 11 running on iPad Pro with Apple A9X CPU without PAA
- iOS 11 running on iPhone 5S with Apple A7 CPU with PAA
- iOS 11 running on iPhone 5S with Apple A7 CPU without PAA
- iOS 11 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU with PAA
- iOS 11 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU without PAA
- iOS 11 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU with PAA
- iOS 11 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU without PAA
- iOS 11 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU with PAA
- iOS 11 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU without PAA
- iOS 11 running on iPhone 8 with Apple A11 Bionic CPU with PAA
- iOS 11 running on iPhone 8 with Apple A11 Bionic CPU without PAA
- tvOS 11 running on Apple TV 4K with Apple A10X Fusion CPU with PAA
- tvOS 11 running on Apple TV 4K with Apple A10X Fusion CPU without PAA
- watchOS 4 running on Apple Watch Series 1 with Apple S1P CPU with PAA

- watchOS 4 running on Apple Watch Series 1 with Apple S1P CPU without PAA
- watchOS 4 running on Apple Watch Series 3 with Apple S3 CPU with PAA
- watchOS 4 running on Apple Watch Series 3 with Apple S3 CPU without PAA

FIPS Algorithms

key establishment methodology provides between 128 and 160 bits of encryption strength

AES	Certs. #4906, #4907, #4908, #4909, #4910, #4911, #4912, #4913, #4916, #4917, #4918, #4919, #4920, #4921, #4922, #4923, #4924, #4925, #4926, #4927, #4928, #4929, #4932, #4935, #5039, #5040, #5041, #5125, #5126, #5127, #5128,

DRBG	Certs. #5129, #5130, #5185, #5186 and #5187 #1736, #1737, #1738, #1739, #1740, #1741, #1742, #1743, #1744, #1745, #1746, #1747, #1748, #1749, #1750, #1751, #1752, #1753, #1754, #1755, #1756, #1757, #1760, #1763, #1849, #1850, #1851, #1852, #1853, #1854, #1855,

	#1856, #1860, #1861, #1862, #1863, #1915, #1916, #1917, #1918, #1919, #1920, #1921, #1922, #1959, #1960, #1961 and #1962
ECDSA	Certs. #1289, #1290, #1291, #1292, #1293, #1294, #1295, #1296, #1298, #1325, #1326 and #1345
HMAC	Certs. #3273, #3274, #3275, #3276, #3277,

	#3278, #3279, #3280, #3350, #3351, #3352, #3353, #3354, #3355, #3356, #3357, #3361, #3362, #3405, #3406, #3407, #3408, #3441 and #3442
KTS	AES Certs. #4906, #4907, #4908, #4909, #4910, #4911, #4912, #4913, #4916, #4917, #4918, #4919, #4920, #4921, #4922, #4923,

	#4924, #4925, #4926, #4927, #4928, #4929, #4932, #4935, #5039, #5040, #5041, #5125, #5126, #5127, #5128, #5129, #5130, #5185, #5186 and #5187
PBKDF	vendor affirmed
RSA	Certs. #2717, #2718, #2719, #2720, #2721, #2722, #2723, #2724, #2728, #2763, #2764 and #2783

SHS	Certs. #4013, #4014, #4015, #4016, #4017, #4018, #4019, #4020, #4095, #4096, #4097, #4098, #4099, #4100, #4101, #4102, #4106, #4107, #4151, #4152, #4153, #4154, #4189 and #4190
Triple-DES	Certs. #2589, #2590, #2595, #2596, #2597, #2598, #2599, #2600, #2602, #2628, #2629

and #2637

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

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications? Subscribe

Information Technology Laboratory

Computer Security Division

TEL: 301.975.8443

Applied Cybersecurity Division

Contact CSRC Webmaster: webmaster-csrc@nist.gov
