Cryptographic Module Validation Program

Certificate #3148

Details

Module Name

Apple CoreCrypto Module v8.0 for ARM

Standard

FIPS 140-2

Status

Active

Sunset Date

3/8/2023

Validation Dates

3/9/2018

5/22/2018

7/6/2018

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 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

AES	Certs. #4862, #4863, #4864, #4865, #4866, #4867, #4868, #4869, #4870, #4871, #4872, #4873, #4874, #4875, #4876, #4877, #4878, #4879, #4880, #4881, #4882, #4883, #4884, #4885, #4886, #4887, #4888, #4889, #4890, #4891, #4892, #4893, #4930, #4931, #4933, #4934, #4936, #4937, #4938, #4939, #4978, #4979, #4980, #4981, #4982, #4983, #4984, #5009, #5013, #5014, #5015, #5016, #5017, #5018, #5082, #5083, #5084, #5085, #5086, #5087, #5088, #5090, #5091, #5092, #5093, #5094, #5171, #5172, #5173, #5174, #5175 and #5176
CVL	Certs. #1522, #1523, #1524, #1525, #1527, #1528, #1529, #1530, #1531, #1532, #1533, #1534, #1535, #1536, #1537, #1538, #1563, #1564, #1637, #1638, #1639, #1640, #1678 and #1679
DRBG	Certs. #1714, #1715, #1716, #1717, #1718, #1719, #1720, #1721, #1722, #1723, #1724, #1725, #1726, #1727, #1728, #1729, #1758, #1759, #1761, #1762, #1764, #1765, #1766, #1767, #1797, #1798, #1799, #1800, #1801, #1802, #1803, #1829, #1830, #1831, #1832, #1833, #1891, #1892, #1893, #1894, #1897, #1898, #1899, #1900, #1949, #1950, #1951 and #1952
ECDSA	Certs. #1255, #1256, #1257, #1258, #1259, #1260, #1261, #1262, #1279, #1317, #1318 and #1341
HMAC	Certs. #3259, #3260, #3261, #3262, #3263, #3264, #3265, #3266, #3281, #3282, #3283, #3284, #3285, #3286, #3287, #3288, #3331, #3332, #3390, #3391, #3395, #3396, #3432 and #3433

KTS	AES Certs. #4870, #4871, #4872, #4873, #4874, #4875, #4876, #4877, #4878, #4879, #4880, #4881, #4882, #4883, #4884, #4885, #4886, #4887, #4888, #4889, #4890, #4891, #4892, #4893, #4930, #4931, #4933, #4934, #4936, #4937, #4938, #4939, #4978, #4979, #4980, #4981, #4982, #4983, #4984, #5009, #5014, #5015, #5016, #5017, #5018, #5084, #5085, #5086, #5087, #5088, #5090, #5091, #5092, #5093, #5094, #5172, #5173, #5174, #5175 and #5176; key establishment methodology provides between 128 and 160 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed
RSA	Certs. #2679, #2680, #2681, #2682, #2683, #2684, #2685, #2686, #2705, #2754, #2755 and #2779
SHS	Certs. #4000, #4001, #4002, #4003, #4004, #4005, #4006, #4007, #4021, #4022, #4023, #4024, #4025, #4026, #4027, #4028, #4076, #4077, #4136, #4137, #4141, #4142, #4180 and #4181
Triple-DES	Certs. #2560, #2561, #2562, #2563, #2564, #2565, #2566, #2567, #2586, #2620, #2621 and #2634

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); 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

Technologies
Sectors
Laws & Regulations
Activities & Products

NEWS & UPDATES

EVENTS

GLOSSARY

ABOUT CSRC
Computer Security Division
Applied Cybersecurity Division
Contact Us

Information Technology Laboratory

Computer Security Division
TEL: 301.975.8443
Applied Cybersecurity Division

Contact CSRC Webmaster: webmaster-csrc@nist.gov
