

[Information Technology Laboratory](#)**COMPUTER SECURITY RESOURCE CENTER**

PROJECTS

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

Cryptographic Module Validation Program



Certificate #3438

Details

| | |
|---------------------------|--|
| Module Name | Apple CoreCrypto Kernel Module v9.0 for ARM |
| Standard | FIPS 140-2 |
| Status | Active |
| Sunset Date | 4/22/2024 |
| Validation Dates | 4/23/2019 |
| Overall Level | 1 |
| Caveat | When operated in FIPS Mode. The module generates cryptographic keys whose strengths are modified by available entropy |
| Security Level Exceptions | <ul style="list-style-type: none"> Physical Security: N/A |
| Module Type | Software |
| Embodiment | Multi-Chip Stand Alone |
| Description | The Apple CoreCrypto Kernel Module v9.0 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) | <ul style="list-style-type: none"> iOS 12 running on iPad Air 2 with Apple A8X CPU with PAA iOS 12 running on iPad Air 2 with Apple A8X CPU without PAA iOS 12 running on iPad Pro with Apple A10X Fusion CPU with PAA iOS 12 running on iPad Pro with Apple A10X Fusion CPU without PAA iOS 12 running on iPad Pro with Apple A12X Bionic CPU with PAA iOS 12 running on iPad Pro with Apple A12X Bionic CPU without PAA iOS 12 running on iPad Pro with Apple A9X CPU with PAA iOS 12 running on iPad Pro with Apple A9X CPU without PAA iOS 12 running on iPhone 5S with Apple A7 CPU with PAA iOS 12 running on iPhone 5S with Apple A7 CPU without PAA iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU with PAA iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU without PAA iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU with PAA iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU without PAA iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU with PAA iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU without PAA iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus) and iPhone X with Apple A11 Bionic CPU with PAA iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus) and iPhone X with Apple A11 Bionic CPU without PAA iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU with PAA |

- iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU without PAA
- tvOS 12 running on Apple TV 4K with Apple A10X Fusion CPU with PAA
- tvOS 12 running on Apple TV 4K with Apple A10X Fusion CPU without PAA
- TxFW 16P374 running on Apple iMac Pro with Apple T2 with PAA
- TxFW 16P374 running on Apple iMac Pro with Apple T2 without PAA
- TxFW 16P374 running on Apple MacBook Pro with Apple T2 with PAA
- TxFW 16P374 running on Apple MacBook Pro with Apple T2 without PAA (single-user mode)
- watchOS 5 running on Apple Watch Series 1 with Apple S1P CPU with PAA
- watchOS 5 running on Apple Watch Series 1 with Apple S1P CPU without PAA
- watchOS 5 running on Apple Watch Series 3 with Apple S3 CPU with PAA
- watchOS 5 running on Apple Watch Series 3 with Apple S3 CPU without PAA
- watchOS 5 running on Apple Watch Series 4 with Apple S4 CPU with PAA
- watchOS 5 running on Apple Watch Series 4 with Apple S4 CPU without PAA

FIPS Algorithms

| | |
|------------|--|
| AES | Certs. #5741, #5742, #5743, #5744, #5745, #5746, #5747, #5748, #5750, #5751, #5752, #5753, #5754, #5755, #5756, #5757, #5758, #5759, #5760, #5761, #5762, #5763, #5764, #5765, #5883, #5884, #5885, #C 19, #C 103, #C 104, #C 147, #C 149, #C 150, #C 178, #C 179, #C 182, #C 183, #C 184, #C 185, #C 249, #C 252, #C 254, #C 255, #C 257 and #C 434 |
| DRBG | Certs. #2336, #2337, #2338, #2339, #2340, #2341, #2342, #2343, #2345, #2346, #2347, #2348, #2349, #2350, #2351, #2352, #2353, #2354, #2355, #2356, #2357, #2358, #2359, #2360, #2446, #2447, #2448, #C 20, #C 103, #C 104, #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 147, #C 149, #C 178, #C 179, #C 180, #C 181, #C 184, #C 185, #C 198, #C 209, #C 248, #C 249, #C 250, #C 251, #C 252, #C 253, #C 255, #C 256, #C 434, #C 437 and #C 438 |
| ECDSA | Certs. #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 209, #C 248, #C 250, #C 251, #C 437 and #C 438 |
| HMAC | Certs. #3806, #3807, #3808, #3809, #3810, #3811, #3812, #3813, #3862, #C 20, #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 180, #C 181, #C 198, #C 209, #C 248, #C 250, #C 251, #C 253, #C 256, #C 437 and #C 438 |
| KTS | AES Certs. #5741, #5742, #5743, #5744, #5745, #5746, #5747, #5748, #5883, #C 103, #C 147, #C 184, #C 185, #C 249 and #C 434; key establishment methodology provides between 128 and 256 bits of encryption strength |
| PBKDF | vendor affirmed |
| RSA | Certs. #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 209, #C 248, #C 250, #C 251, #C 437 and #C 438 |
| SHS | Certs. #4579, #4580, #4581, #4582, #4583, #4584, #4585, #4586, #4637, #C 20, #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 180, #C 181, #C 198, #C 209, #C 248, #C 250, #C 251, #C 253, #C 256, #C 437 and #C 438 |
| Triple-DES | Certs. #C 127, #C 128, #C 129, #C 130, #C 131, #C 132, #C 133, #C 134, #C 135, #C 209, #C 248, #C 250, #C 251, #C 437 and #C 438 |

| | |
|--------------------|---|
| Allowed Algorithms | MD5; NDRNG; RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength) |
| Software Versions | 9.0 |
| Product URL | http://support.apple.com/en-us/HT202739 |

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

| |
|---------------------------------|
| Related Files |
| Security Policy |
| Lab |

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

ATSEC INFORMATION SECURITY CORP
 NVLAP Code: 200658-0



HEADQUARTERS
 100 Bureau Drive
 Gaithersburg, MD 20899

Want updates about CSRC and our publications? [Subscribe](#)

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

PROJECTS

PUBLICATIONS

Draft Pubs

Final Pubs

FIPS

Special Publications (SPs)

NISTIRs

ITL Bulletins

White Papers

Journal Articles

Conference Papers

Books

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 Technology Laboratory (ITL)

Computer Security Division (CSD)

TEL: 301.975.8443

Applied Cybersecurity Division (ACD)

Contact CSRC Webmaster:

webmaster-csrc@nist.gov

[Privacy Statement](#) | [Privacy Policy](#) | [Security Notice](#) | [Accessibility Statement](#) | [NIST Privacy Program](#) | [No Fear Act Policy](#)

[Disclaimer](#) | [FOIA](#) | [Environmental Policy Statement](#) | [Cookie Disclaimer](#) | [Scientific Integrity Summary](#) | [NIST Information Quality Standards](#)

[Business USA](#) | [Commerce.gov](#) | [Healthcare.gov](#) | [Science.gov](#) | [USA.gov](#)