

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

PROJECTS

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

# Cryptographic Module Validation Program



## Certificate #3433

### Details

Module Name	Apple CoreCrypto Module v9.0 for ARM
Standard	FIPS 140-2
Status	Active
Sunset Date	4/10/2024
Validation Dates	4/11/2019
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"> <li>Physical Security: N/A</li> </ul>
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	The Apple CoreCrypto 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"> <li>iOS 12 running on iPad Air 2 with Apple A8X CPU with PAA</li> <li>iOS 12 running on iPad Air 2 with Apple A8X CPU without PAA</li> <li>iOS 12 running on iPad Pro with Apple A10X Fusion CPU with PAA</li> <li>iOS 12 running on iPad Pro with Apple A10X Fusion CPU without PAA</li> <li>iOS 12 running on iPad Pro with Apple A12X Bionic CPU with PAA</li> <li>iOS 12 running on iPad Pro with Apple A12X Bionic CPU without PAA</li> <li>iOS 12 running on iPad Pro with Apple A9X CPU with PAA</li> <li>iOS 12 running on iPad Pro with Apple A9X CPU without PAA</li> <li>iOS 12 running on iPhone 5S with Apple A7 CPU with PAA</li> <li>iOS 12 running on iPhone 5S with Apple A7 CPU without PAA</li> <li>iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU with PAA</li> <li>iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU without PAA</li> <li>iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU with PAA</li> <li>iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU without PAA</li> <li>iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU with PAA</li> <li>iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU without PAA</li> <li>iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus and iPhone X) with Apple A11 Bionic CPU with PAA</li> <li>iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus and iPhone X) with Apple A11 Bionic CPU without PAA</li> <li>iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU with PAA</li> </ul>

- 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. #5701, #5702, #5703, #5704, #5705, #5706, #5707, #5708, #5709, #5710, #5711, #5712, #5713, #5714, #5715, #5716, #5717, #5718, #5719, #5720, #5721, #5722, #5723, #5724, #5725, #5726, #5727, #5728, #5729, #5730, #5731, #5732, #5733, #5734, #5735, #5736, #5737, #5738, #5739, #5740, #5836, #5837, #5838, #5839, #5840, #5841, #5842, #5843, #5844, #5845, #5879, #5880, #5881, #5882, #5886, #C10, #C11, #C12, #C13, #C14, #C15, #C16, #C25, #C26, #C27, #C28, #C29, #C30, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C105, #C106, #C107, #C145, #C146, #C148, #C239, #C240, #C241, #C242, #C243, #C245, #C246 and #C247
CVL	Certs. #2115, #2180, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243 and #C245
DRBG	Certs. #2312, #2313, #2314, #2315, #2316, #2317, #2318, #2319, #2320, #2321, #2322, #2323, #2324, #2325, #2326, #2327, #2328, #2329, #2330, #2331, #2332, #2333, #2334, #2335, #2429, #2430, #2431, #2432, #2433, #2434, #2443, #2444, #2445, #2449, #C13, #C16, #C29, #C30, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C105, #C106, #C107, #C145, #C146, #C148, #C239, #C240, #C241, #C242, #C243, #C245, #C246 and #C247
DSA	Certs. #1481 and #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243, #C245
ECDSA	Certs. #1567, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243, #C245
HMAC	Certs. #3798, #3799, #3800, #3801, #3802, #3803, #3804, #3805, #3856, #3857, #3861, #3863, #C13, #C16, #C29, #C30, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243 and #C245
KTS	AES Certs. #5701, #5702, #5703, #5704, #5705, #5706, #5707, #5716, #5836, #5841, #5879, #5886, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C106, #C107, #C146, #C148, #C239, #C240, #C241, #C242, #C243 and #C245; key establishment methodology provides 128 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed
RSA	Certs. #3084, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243 and #C245
SHS	Certs. #4571, #4572, #4573, #4574, #4575, #4576, #4577, #4578, #4631, #4632, #4636, #4638, #C13, #C16, #C29, #C30, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243 and #C245
Triple-DES	Certs. #2866, #C95, #C96, #C97, #C98, #C99, #C100, #C101, #C102, #C107, #C148, #C239, #C242, #C243 and #C245

Allowed Algorithms

Diffie-Hellman (CVL Certs. #2115, #C 95, #C 96, #C 97, #C 98, #C 99, #C 100, #C 101, #C 102, #C 107, #C 148, #C 239, #C 242, #C 243, #C 245, key agreement; key establishment methodology provides 112 or 128 bits of encryption

strength); EC Diffie-Hellman (CVL Certs. #2115, #C 95, #C 96, #C 97, #C 98, #C 99, #C 100, #C 101, #C 102, #C 107, #C 148, #C 239, #C 242, #C 243, #C 245, key agreement; key establishment methodology provides 128 bits of encryption strength); MD5; NDRNG; RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

Software Versions

9.0

**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

**Lab**

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](#)