Cryptographic Module Validation Program

Certificate #2827

Details

Module Name
Apple iOS CoreCrypto Module v7.0

Standard
FIPS 140-2

Status
Active

Sunset Date

1/31/2022

Validation Dates

2/1/2017

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 iOS CoreCrypto Module is a software cryptographic module running on a multi-chip standalone mobile device and provides services intended to protect data in transit and at rest.

Tested Configuration(s)

- iOS 10.2 running on iPad Air 2 with Apple A8X CPU
- iOS 10.2 running on iPad Pro with Apple A9X CPU (single-user mode)
- iOS 10.2 running on iPhone5S with Apple A7 CPU
- iOS 10.2 running on iPhone6 (iPhone6 and iPhone6 Plus) with Apple A8 CPU
- iOS 10.2 running on iPhone6S (iPhone6S and iPhone6S Plus) with Apple A9 CPU
- iOS 10.2 running on iPhone7 (iPhone7 and iPhone7 Plus) with Apple A10

CPU

FIPS Algorithms

AES	Certs. #4156, #4157, #4158, #4159, #4160, #4161, #4162, #4163, #4164, #4165, #4166, #4167, #4168, #4169, #4170, #4171, #4172, #4173, #4174, #4175, #4176, #4177, #4178, #4179, #4180, #4181, #4182, #4183, #4184, #4185, #4186, #4187, #4188, #4189, #4190 and #4269
CVL	Certs. #959, #960, #961, #962, #963, #964, #965, #966, #967, #968, #969 and #1010
DRBG	Certs. #1264, #1265, #1266, #1267, #1268, #1269, #1270, #1271, #1272, #1273, #1274, #1275, #1276, #1277, #1278, #1279, #1280, #1281, #1282, #1283, #1284, #1285, #1286 and #1339
ECDSA	Certs. #957, #958, #959, #960, #961, #962, #963, #964, #965, #966, #967 and #997
HMAC	Certs. #2723, #2724, #2725, #2726, #2727, #2728, #2729, #2730, #2731, #2732, #2733, #2734, #2735, #2736, #2737, #2738, #2739, #2740, #2741, #2742, #2743, #2744, #2745 and #2813
KTS	AES Certs. #4156, #4157, #4158, #4159, #4160, #4161, #4162, #4163, #4164, #4166, #4169, #4170, #4180, #4181, #4182, #4183, #4184, #4185, #4186, #4187, #4188, #4189, #4190 and #4269; key establishment methodology provides between 128 and 160 bits of encryption strength
KTS	vendor affirmed
PBKDF	vendor affirmed

RSA	Certs. #2264, #2265, #2266, #2267, #2268, #2269, #2270, #2271, #2272, #2273, #2274 and #2299
SHS	Certs. #3421, #3422, #3423, #3424, #3425, #3426, #3427, #3428, #3429, #3430, #3431, #3432, #3433, #3434, #3435, #3436, #3437, #3438, #3439, #3440, #3441, #3442, #3443 and #3514
Triple-DES	Certs. #2272, #2273, #2274, #2275, #2276, #2277, #2278, #2279, #2280, #2281, #2282 and #2308

Other Algorithms

Diffie-Hellman (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 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; non-compliant less than 112 bits of encryption strength); AES-CMAC (non-compliant); ANSI X9.63 KDF; Blowfish; CAST5; DES; ECDSA (non-compliant); Ed25519; Hash_DRBG (non-compliant); Integrated Encryption Scheme on elliptic curves; KBKDF (non-compliant); MD2; MD4; MD5; OMAC (One-Key CBC MAC); RFC6637 KDF; RIPEMD; RC2; RC4; RSA (non-compliant); SP800-56C KDF (non-compliant); Triple-DES (non-compliant)

Software Versions

7.0

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 CORPORATION
NVLAP Code: 200658-0

Want updates about CSRC and our publications?

Subscribe

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

Information Technology Laboratory

Computer Security Division
TEL: 301.975.8443
Applied Cybersecurity Division

Contact CSRC Webmaster: webmaster-csrc@nist.gov
