Cryptographic Module Validation Program

Certificate #2828

Details

Module Name
Apple iOS CoreCrypto Kernel 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 Kernel 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. #4255, #4256, #4257, #4258, #4259, #4260, #4293, #4294, #4295, #4296, #4297 and #4298
DRBG	Certs. #1353, #1354, #1355, #1356, #1357 and #1358
ECDSA	Certs. #1003, #1004, #1005, #1006, #1007 and #1008
HMAC	Certs. #2829, #2830, #2831, #2832, #2833, #2834, #2854, #2855, #2856, #2857, #2858 and #2859
KTS	AES Certs. #4255, #4256, #4257, #4258, #4259, #4260, #4293, #4294, #4295, #4296, #4297 and #4298; key establishment methodology provides between 128 and 160 bits of encryption strength
PBKDF	vendor affirmed
RSA	Certs. #2314, #2315, #2316, #2317, #2318 and #2319
SHS	Certs. #3531, #3532, #3533, #3534, #3535, #3536, #3557, #3558, #3559, #3560, #3561 and #3562
Triple-DES	Certs. #2314, #2315, #2316, #2317, #2318 and #2319

Other Algorithms

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 (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); RC2; RC4; RFC6637 KDF; RIPEMD; 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

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