Cryptographic Module Validation Program CMVP

Certificate #3811

Details

Module Name	Apple Secure Key Store Cryptographic Module, v10.0
Standard	FIPS 140-2
Status	Active
Sunset Date	2/4/2026
Validation Dates	02/05/2021
Overall Level	2
Caveat	When operated in FIPS mode
Security Level Exceptions	• Mitigation of Other Attacks: N/A
Module Type	Hardware
Embodiment	Single Chip
Description	The Apple Secure Key Store Cryptographic Module is a single-chip standalone hardware cryptographic module running on a multi-chip device and provides services intended to protect data in transit and at rest.
Tested Configuration(s)	• SEPOS distributed with iOS 13 running on iPhone 11 Pro Max with Apple A13 Bionic [2] • SEPOS distributed with iOS 13 running on iPhone 6S Plus with Apple A9 [2] • SEPOS distributed with iOS 13 running on iPhone 7 Plus with Apple A10 Fusion [2] • SEPOS distributed with iOS 13 running on iPhone 8 Plus with Apple A11 Bionic [2] • SEPOS distributed with iOS 13 running on iPhone Xs Max with Apple A12 Bionic [2] • SEPOS distributed with iPadOS 13 running on iPad (5th generation) with Apple A9 [2] • SEPOS distributed with iPadOS 13 running on iPad (6th generation) with Apple A10 Fusion [2] • SEPOS distributed with iPadOS 13 running on iPad Air 2 with Apple A8X [1] • SEPOS distributed with iPadOS 13 running on iPad mini (5th generation) with Apple A12 Bionic [2] • SEPOS distributed with iPadOS 13 running on iPad mini 4 with Apple A8 [1] • SEPOS distributed with iPadOS 13 running on iPad Pro (12.9 inch, 2nd generation) with Apple A10X Fusion [2] • SEPOS distributed with iPadOS 13 running on iPad Pro (12.9 inch, 3rd generation) with Apple A12X Bionic [2] • SEPOS distributed with iPadOS 13 running on iPad Pro (9.7 inch) with Apple A9X [2] • SEPOS distributed with tvOS 13 running on Apple TV 4K with Apple A10X Fusion [2] • SEPOS distributed with TxFW 10.15 running on Apple T2 [2] • SEPOS distributed with watchOS 6 running on Apple Watch Series 1 with Apple S1P [2] • SEPOS distributed with watchOS 6 running on Apple Watch Series 3 with Apple S3 [2] • SEPOS distributed with watchOS 6 running on Apple Watch Series 4 with Apple S4 [2] • SEPOS distributed with watchOS 6 running on Apple Watch Series 5 with Apple S5 [2]

FIPS Algorithms

AES	Certs. #5261, #5270, #5271, #5272, #5273, #5274, #5275, #5276, #5278, #5279, #A494, #A496, #A497, #A498, #A499, #A501, #A510, #C312, #C313, #C314, #C315, #C317, #C318, #C319, #C320, #C322, #C323, #C324, #C325, #C326, #C330, #C331 and #C358
CKG	vendor affirmed
DRBG	Certs. #2014, #2020, #2021, #2022, #2023, #2024, #2025, #2026, #2028, #2029, #A501, #C323, #C324 and #C331
ECDSA	Cert. #A495
HMAC	Certs. #A495, #A497 and #A500
KAS-SSC	vendor affirmed
KTS	AES Certs. #A497 and #A498; key establishment methodology provides between 128 and 256 bits of encryption strength
PBKDF	vendor affirmed
SHS	Certs. #A495, #A497 and #A500

Allowed Algorithms	NDRNG
Hardware Versions	1.2[1], 2.0[2]
Firmware Versions	SEPOS
Product URL	http://support.apple.com/en-us/HT202739

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
Fiona Pattinson
fpattison@apple.com
Phone: 512-825-3083

Related Files

Security Policy

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0

NIST National Institute of Standards and Technology U.S. Department of Commerce

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications? Subscribe

Webmaster | Contact Us | Our Other Offices

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 | Commerce.gov | Healthcare.gov | Science.gov | USA.gov