Cryptographic Module Validation Program

Certificate #3223

Details

Module Name

Apple Secure Key Store Cryptographic Module, v1.0

Standard

FIPS 140-2

Status

Active

Sunset Date

7/9/2023

Validation Dates

7/10/2018

Overall Level

1

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 running on Apple iMac Pro 2017 with Apple iBridge2,1 CPU [2] (single-user mode)
- SEPOS running on Apple TV 4K with Apple A10X Fusion CPU[2]
- SEPOS running on Apple Watch Series 1 with Apple S1P CPU[2]
- SEPOS running on Apple Watch Series 3 with Apple S3 CPU[2]
- SEPOS running on iPad Air 2 with Apple A8X CPU[1]
- SEPOS running on iPad Pro with Apple A9X CPU[2], SEPOS running on iPad Pro with Apple A10X Fusion CPU[2]

- SEPOS running on iPhone 5S with Apple A7 CPU[1]
- SEPOS running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU[1]
- SEPOS running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU[2]
- SEPOS running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU[2]
- SEPOS running on iPhone 8 and iPhone X (iPhone 8, iPhone 8 Plus, iPhone X) with Apple A11 Bionic CPU[2]

FIPS Algorithms

AES	Certs. #5102, #5103, #5104, #5105, #5106, #5107, #5108, #5109, #5110, #5111, #5112, #5113, #5114, #5115, #5116, #5117, #5118, #5119, #5120, #5121, #5131, #5132, #5133, #5134, #5135, #5136, #5137, #5138, #5139, #5140, #5141, #5142, #5143, #5144, #5145, #5146, #5147, #5148, #5149, #5150, #5151, #5152, #5153, #5154, #5155, #5156, #5157, #5159, #5160, #5161, #5162, #5163, #5164, #5165, #5182, #5188, #5189, #5190, #5191, #5192, #5193, #5194, #5195, #5196, #5197, #5198, #5199, #5200, #5201, #5202, #5213, #5214, #5215, #5216 #5217, #5218, #5219, #5220, #5221, #5222, #5223, #5224, #5225, #5226, #5260, #5261, #5270, #5271, #5272, #5273, #5274, #5275, #5276, #5277, #5278 and #5279
CKG	vendor affirmed
CVL	Certs. #1654, #1656, #1658, #1660, #1662, #1664, #1666, #1668, #1670, #1686, #1696 and #1698
DRBG	Certs. #2013, #2014, #2020, #2021, #2022, #2023, #2024, #2025, #2026, #2027, #2028 and #2029
ECDSA	Certs. #1327, #1328, #1329, #1330, #1331, #1332, #1333, #1334,

	#1335, #1346, #1351 and #1352
HMAC	Certs. #3409, #3410, #3411, #3412, #3413, #3414, #3415, #3416, #3417, #3418, #3420, #3421, #3422, #3423, #3424, #3425, #3426, #3438, #3443, #3444, #3455, #3456, #3457 and #3458
KTS	AES Certs. #5102, #5103, #5106, #5110, #5113, #5114, #5115, #5116, #5117, #5118, #5119, #5120, #5121, #5131, #5132, #5133, #5143, #5145, #5146, #5148, #5149, #5150, #5151, #5152, #5153, #5154, #5155, #5156, #5157, #5159, #5160, #5161, #5162, #5163, #5164, #5165, #5182, #5188, #5189, #5190, #5191, #5192, #5193, #5194, #5195, #5198, #5199, #5200, #5201, #5202, #5215, #5216, #5217, #5219, #5221, #5222, #5223, #5224, #5225 and #5226; key establishment methodology provides between 128 and 256 bits of encryption strength
PBKDF	vendor affirmed
SHS	Certs. #4155, #4156, #4157, #4158, #4159, #4160, #4161, #4162, #4163, #4164, #4166, #4167, #4168, #4169, #4170, #4171, #4172, #4186, #4191, #4192, #4203, #4204, #4205 and #4206

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.
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 CORP
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
