

Information Technology Laboratory



# COMPUTER SECURITY RESOURCE CENTER



PROJECTS

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

## Cryptographic Module Validation Program



### Certificate #3523

#### Details

Module Name	Apple Secure Key Store Cryptographic Module, v9.0
Standard	FIPS 140-2
Status	Active
Sunset Date	9/9/2024
Validation Dates	9/10/2019
Overall Level	2
Caveat	When operated in FIPS mode
Security Level Exceptions	<ul style="list-style-type: none"> <li>Mitigation of Other Attacks: N/A</li> </ul>
Module Type	Hardware
Embodiment	Single Chip
Description	The Apple Secure Key Store Cryptographic Module, v9.0 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)	<ul style="list-style-type: none"> <li>SEPOS running on Apple iMac Pro 2017 with Apple T2 CPU[2]</li> <li>SEPOS running on Apple MacBook Pro with Apple T2 CPU[2]</li> <li>SEPOS running on Apple TV 4K with Apple A10X Fusion CPU[2]</li> <li>SEPOS running on Apple Watch Series 1 with Apple S1P CPU[2]</li> <li>SEPOS running on Apple Watch Series 3 with Apple S3 CPU[2]</li> <li>SEPOS running on Apple Watch Series 4 with Apple S4 CPU[2]</li> <li>SEPOS running on iPad Air 2 with Apple A8X CPU[1]</li> <li>SEPOS running on iPad Pro with Apple A12X Bionic CPU[2]</li> <li>SEPOS running on iPad Pro with Apple A9X CPU[2], SEPOS running on iPad Pro with Apple A10X Fusion CPU[2]</li> <li>SEPOS running on iPhone 5S with Apple A7 CPU[1]</li> <li>SEPOS running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU[1]</li> <li>SEPOS running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU[2]</li> <li>SEPOS running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU[2]</li> <li>SEPOS running on iPhone 8 and iPhone X (iPhone 8, iPhone 8 Plus, iPhone X) with Apple A11 Bionic CPU[2]</li> <li>SEPOS running on iPhone XS (iPhone XS, iPhone XS Max, iPhone XR) with Apple A12 Bionic CPU[2]</li> </ul>
FIPS Algorithms	<p>AES Certs. <a href="#">#5260</a>, <a href="#">#5261</a>, <a href="#">#5270</a>, <a href="#">#5271</a>, <a href="#">#5272</a>, <a href="#">#5273</a>, <a href="#">#5274</a>, <a href="#">#5275</a>, <a href="#">#5276</a>, <a href="#">#5278</a>, <a href="#">#5279</a>, <a href="#">#C87</a>, <a href="#">#C88</a>, <a href="#">#C89</a>, <a href="#">#C90</a>, <a href="#">#C91</a>, <a href="#">#C92</a>, <a href="#">#C93</a>, <a href="#">#C94</a>, <a href="#">#C151</a>, <a href="#">#C152</a>, <a href="#">#C153</a>, <a href="#">#C154</a>, <a href="#">#C155</a>, <a href="#">#C156</a>, <a href="#">#C157</a>, <a href="#">#C158</a>, <a href="#">#C159</a>, <a href="#">#C160</a>, <a href="#">#C161</a>, <a href="#">#C162</a>, <a href="#">#C163</a>, <a href="#">#C164</a>, <a href="#">#C165</a>, <a href="#">#C166</a>, <a href="#">#C167</a>, <a href="#">#C168</a>, <a href="#">#C169</a>, <a href="#">#C192</a>, <a href="#">#C199</a>, <a href="#">#C200</a>, <a href="#">#C201</a>, <a href="#">#C202</a>, <a href="#">#C203</a>, <a href="#">#C204</a>, <a href="#">#C205</a>, <a href="#">#C206</a>, <a href="#">#C207</a>, <a href="#">#C208</a>, <a href="#">#C258</a>, <a href="#">#C260</a>, <a href="#">#C261</a>, <a href="#">#C262</a>, <a href="#">#C263</a>, <a href="#">#C264</a>, <a href="#">#C265</a>, <a href="#">#C266</a>,</p>

#C267, #C268, #C270, #C271, #C273, #C274, #C275, #C277, #C278, #C279, #C280, #C282, #C283, #C284, #C286, #C288, #C289, #C290, #C291, #C292, #C293, #C294, #C296, #C298, #C299, #C300, #C301, #C305, #C306, #C307, #C308, #C309, #C310, #C311, #C312, #C313, #C314, #C315, #C317, #C318, #C319, #C320, #C322, #C323, #C324, #C325, #C326, #C330, #C331, #C358, #C359, #C360, #C361, #C362, #C363, #C364, #C365, #C366, #C367, #C368 and #C369

- CKG vendor affirmed
- CVL Certs. #C162, #C163, #C164, #C165, #C166, #C167, #C168, #C169, #C258, #C260, #C290, #C296, #C310, #C363 and #C364
- DRBG Certs. #2013, #2014, #2020, #2021, #2022, #2023, #2024, #2025, #2026, #2028, #2029, #C323, #C324 and #C331
- ECDSA Certs. #C162, #C163, #C164, #C165, #C166, #C167, #C168, #C169, #C258, #C260, #C290, #C296, #C310, #C363 and #C364
- HMAC Certs. #C162, #C163, #C164, #C165, #C166, #C167, #C168, #C169, #C258, #C260, #C268, #C270, #C271, #C277, #C278, #C279, #C280, #C282, #C283, #C284, #C290, #C292, #C296, #C300, #C301, #C309, #C310, #C363, #C364 and #C369
- KTS AES Certs. #C87, #C88, #C89, #C90, #C91, #C92, #C93, #C94, #C161, #C162, #C163, #C164, #C165, #C166, #C167, #C168, #C169, #C192, #C258, #C260, #C288, #C290, #C293, #C296, #C306, #C310, #C360, #C362, #C363 and #C364; key establishment methodology provides between 128 and 256 bits of encryption strength
- PBKDF vendor affirmed
- SHS Certs. #C162, #C163, #C164, #C165, #C166, #C167, #C168, #C169, #C258, #C260, #C268, #C270, #C271, #C277, #C278, #C279, #C280, #C282, #C283, #C284, #C290, #C292, #C296, #C300, #C301, #C309, #C310, #C363, #C364 and #C369

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

**Related Files**

[Security Policy](#)  
[Consolidated Certificate](#)

**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](mailto: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](#)