Crypto Officer Role Guide for FIPS 140-2 Compliance

for SEP Secure Key Store

Contents

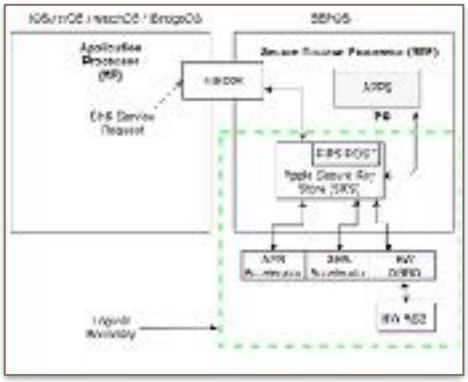
Overview

In highly regulated industries, IT System Administrators and Crypto Officers are frequently required to ensure deployed systems are correctly using FIPS 140-2 Validated Cryptographic Modules. The **Apple Secure Enclave Processor Secure Key Store Cryptographic Module, v1.0** achieved **FIPS 140-2 Conformance Validation** under the Cryptographic Module Validation Program (CMVP) – a joint American and Canadian security accreditation program for cryptographic modules.

The **Apple Secure Enclave Processor (SEP) Secure Key Store (SKS) Cryptographic Module** is a hardware cryptographic module running on a single-chip standalone processor. The module is embedded inside the Secure Enclave Processor (SEP) and packaged within multiple Apple System-On-Chip (SoC) identified as A, S, and T.

Critical cryptographic services provided by the module are:

- random number generation and symmetric key generation
  - *[SP 800-90A, SP 800-133] TRNG: HW DRBG (CTR_DRBG)*
- digital signature and asymmetric key generation
  - *[FIPS 186-4] ECDSA, ANSI X9.62*
- key derivation
  - *[SP 800-132] PBKDF2*
- key agreement
  - *[SP 800-56A] EC DH*
- key wrapping / unwrapping
  - *[SP 800-38F] AES-KW*
- data encryption / decryption
  - *[FIPS 197, SP 800-38A,D,F] AES*
- message digest
  - *[FIPS 180-4] SHS*
- generation of hash values
  - *[FIPS 198] HMAC*
- key zeroization
  - *[SP 800-88] Media Sanitization*


iOS / tvOS / watchOS / BridgeOS
SEPOS
Application Processor (AP)
Secure Enclave Processor (SEP)
SKS Service Request
FIPS POST
Apple Secure Key Store (SKS)
AES Accelerator
SHA Accelerator
HW DRBG
Logical Boundary

The cryptographic module boundary includes a DRBG hardware component with AES and SHA hardware accelerators as part of the module which is integrated into the SoC and is reachable by the SEP execution environment. The module hardware version is v1.2 for hardware DRBG in A7, A8 and A8X SoCs and v2.0 found in all others.

The referenced devices listed in Table 1 and 2 later in this document have an embed SoC which has multiple execution environments, including different CPUs for the main operating systems (iOS, tvOS, watchOS, macOS) and the operating systems driving the Secure Enclave Processor (SEP). Both environments are operating systems executing on different CPUs embedded within the SoC. Both execution environments are separated by the SoC and thus execute independent of each other. The module consists of firmware and a hardware component. The firmware part operates on hardware consistent with that of a GPC.

Validation References and Resources

CMVP

This hardware module is identified under the CMVP with the module name of:

Apple Secure Enclave Processor Secure Key Store Cryptographic Module, v1.0

#3223 Certificate & Security Policy

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3223

csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3223.pdf

All Apple Validated Crypto Modules can be found under CMVP's new FIPS 140-2 Validated Cryptographic Module Search page and searching for 'Vendor:' **Apple**

Active Validation List
https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Archived validations can be found using the 'search type' of ***Advanced*** *and selecting 'Validation Status' of* ***Historical****.*

NOTE: Within this and other Apple documents, those modules may also be referred to by other names such as **"Secure Key Store (SKS)", "SEP Secure Key Store", etc.**

Apple

References to the validated **Apple Secure Enclave Processor Secure Key Store Cryptographic Module, v1.0**, this Crypto Officer Role Guide, links to the Security Policy document and CMVP issued certificate can be found in each of the corresponding OS Knowledge Base Articles -

Product security certifications, validations, and guidance for …

macOS	https://support.apple.com/en-us/HT201159
iOS	https://support.apple.com/en-us/HT202739
tvOS	https://support.apple.com/en-us/HT208389
watchOS	https://support.apple.com/en-us/HT208390
T2 Firmware	https://support.apple.com/en-us/HT208675

Compliant Services

Compliancy Requirements on Crypto Officers are not limited to the use of products containing a validated cryptographic module, but extend to their attestation that applications and services in use are FIPS 140-2 Compliant. Compliance is defined by CMVP to include both the use of a FIPS 140-2 validated module and the proper use of FIPS-Approved Algorithms.

Services

The **Apple Secure Enclave Processor Secure Key Store Cryptographic Module** provides cryptographic services from within the Secure Enclave Processor (SEP) to the underlying Apple SoC and the SEP OS. There is no direct access from third-party applications running on the platform operating system.

A high-level, non-exhaustive list of built-in services that use the Secure Key Store (SKS) that are FIPS 140-2 Compliant for all validated platforms would start with the following:

- Unlock of device or account *(Password & Biometric)*
- Hardware Encryption / Data Protection / FileVault *(Data-at-Rest)*
- Secure Boot *(Firmware and OS Trust and Integrity)*
- Hardware control of camera *(FaceTime)*

Third-party developers can:

- request non-extractable keys be created in and protected by the Secure Enclave

Other platform services would be handled by either of the two FIPS 140 validated cryptographic modules identified as **Apple CoreCrypto Module v8 for ARM** (User Space) and **Apple CoreCrypto Kernel Module v8 for ARM** (Kernel Space).

Developer and Crypto Officer Resources

There are many resources available to developers providing guidance on cryptographic services and API documentation. Developers should refer to these resources to ensure their products and services are **FIPS 140-2 Compliant** on the corresponding operating system.

Crypto Officer Role Guide

This document provides IT System Administrators with the necessary technical information to ensure FIPS 140-2 compliance of the systems. This guide walks the reader through the system's assertion of cryptographic module integrity and the steps necessary if module integrity requires remediation. A link to the Guides can be found on the Product security certifications, validations, and guidance Knowledge Base Articles listed earlier in this document.

Storing Keys in the Secure Enclave

The Secure Enclave is a hardware-based key manager that's isolated from the main processor to provide an extra layer of security. When you store a private key in the Secure Enclave, you never actually handle the key, making it difficult for the key to become compromised. Instead, you instruct the Secure Enclave to create the key, securely store it, and perform operations with it. You receive only the output of these operations, such as encrypted data or a cryptographic signature verification outcome.

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave

Certificate, Key, and Trust Services Programming Guide

https://developer.apple.com/library/ios/documentation/Security/Conceptual/CertKeyTrustProgGuide/

Security Overview

https://developer.apple.com/library/ios/documentation/Security/Conceptual/Security_Overview/Introduction/Introduction.html

Cryptographic Services Guide

https://developer.apple.com/library/ios/documentation/Security/Conceptual/Security_Overview/CryptographicServices/CryptographicServices.html

Generating New Cryptographic Keys

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/generating_new_cryptographic_keys

Storing Keys in the Keychains

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_keychain

Operationally Tested Platforms

During the validation process for FIPS 140-2 Conformance, the cryptographic module is put through operational testing environments on all the evaluated platforms and noted on the issued certificate. Compliant platforms are Apple systems with a SoC identified as A7 through A11 Bionic, S1P, S3, and T2.

The **Apple Secure Enclave Processor Secure Key Store Cryptographic Module, v1.0** was validated using each platform under the following operational testing environments:

Table 1: Operational Testing Platforms

SoC	SEP OS for SoC **w/OS**	**Device(s)**
A7	iOS 11	iPhone 5s
A8	iOS 11	iPhone 6
A8X	iOS 11	iPad Air 2
A9	iOS 11	iPhone 6s
A9X	iOS 11	iPad Pro 12.9-inch
A10 Fusion	iOS 11	iPhone 7
A10X Fusion	iOS 11	iPad Pro 12.9-inch (2nd gen)
A11 Bionic	iOS 11	iPhone 8 & iPhone X
A10X Fusion	tvOS 11	Apple TV 4K
S1P	watchOS 4	Apple Watch Series 1
S3	watchOS 4	Apple Watch Series 3
T2 (iBridge2,1)	T2 Firmware (15P2064)	iMac Pro (2017)

Compliant Platforms

For FIPS 140-2 Compliance, the platforms noted above articulate Apple systems which were used specifically for the operational testing of the hardware cryptographic module. The full list of **FIPS 140-2 compliant platforms** containing the **FIPS 140-2 validated hardware module** as of **March 2018** are listed below and at the corresponding links:

Table 2: FIPS 140-2 Compliant Platforms

iOS 11	https://support.apple.com/KM207938		
	iPhone X	iPad Pro 12.9-inch (2nd gen)	iPod touch (6th gen)
	iPhone 8 Plus	iPad Pro 10.5-inch	
	iPhone 8	iPad Pro 12.9-inch	
	iPhone 7 Plus	iPad Pro 9.7-inch	
	iPhone 7	iPad Air 2	
	iPhone 6s Plus	iPad Air	
	iPhone 6s	iPad mini 4	
	iPhone SE	iPad mini 3	
	iPhone 6 Plus	iPad mini 2	
	iPhone 6		
	iPhone 5s		
tvOS 11	https://www.apple.com/apple-tv-4k/		
	AppleTV 4K		
watchOS 4	https://www.apple.com/watchos/		
	Apple Watch Series 1		
	Apple Watch Series 3		
T2	https://www.apple.com/imac-pro/		
	iMac Pro		

“FIPS Mode” automatic

“FIPS Mode” is enabled all the time automatically without the need for installation, administration or configuration. All instances of iOS 11, tvOS 11, watchOS 4, and T2 Firmware are using the Secure Key Store (SKS) validated cryptographic module and are enforcing the required module operational and algorithm tests.

These systems will perform all required tests such as the Power-On-Self-Tests (POST), integrity tests on the algorithms and module components, pairwise consistency tests, and finally the conditional self-tests on the random number generator according to the **FIPS 140-2 Level 1 Conformance Validation**.

The FIPS Power-On-Self-Test (POST) process flow

1. Apple system is physically Powered on

2. Operating System begins the bootstrap process

3. Operating System ensures integrity of the **Secure Key Store Cryptographic Module**

    3.1. Validation
    - 3.1.1. The SEP OS determines hardware operating environment (i.e arm64)
    - 3.1.2. The SEP OS reads a validated HMAC_SHA256 for the SKS Module
    - 3.1.3. The SKS Module is started and provided the correct validated HMAC from 3.1.2
    - 3.1.4. The SKS Module will generate an HMAC_SHA256 of the SKS Module code and compare the result against the validated HMAC_SHA256 from 3.1.2
    - 3.1.5. If the calculated HMAC_SHA256 does not match the validated HMAC_SHA256, the system will panic and halt

    3.2. The cipher Power-On-Self-Test (POST) validates the algorithms and modes
    - 3.2.1. The SKS Module performs POST on algorithms and modes *(HW & SW)*
    - 3.2.2. If any part of the POST fails, the system will panic and halt

4. Halt upon failure of any tests on the **Secure Key Store Cryptographic Module**

    4.1. If any phase or step of testing components fails, the system will log the failure and panic and halt the device immediately.

How to verify integrity of the module

A boot-up of the device always forces the FIPS POST which verifies the integrity of the **Secure Key Store (SKS) Cryptographic Hardware Module** prior to processing any cryptographic material. If the device boots-up successfully, the module has passed all FIPS POST verification tests. If the device halts or shuts down during boot-up, an integrity issue has been found during the POST process.

Rebooting the device will always force FIPS POST verification of the SKS hardware cryptographic module.

How to mitigate integrity issues of the module

If a crypto module integrity issue has been identified during the FIPS POST, the only recourse the Crypto Office has for mitigation is to re-install the OS on the device.

If the Crypto Officer needs assistance in restoring the OS Software, relevant Apple Knowledge Base Articles should prove to be quite helpful.

A few helpful support articles available from the Apple Support Knowledge Base:

- **Update your iPhone, iPad, or iPod touch**

  https://support.apple.com/en-us/HT204204

- **Update the software on your Apple TV**

  https://support.apple.com/en-us/HT202716

- **Update your Apple watch**

  https://support.apple.com/en-us/HT204641

- **How to reinstall macOS**

  https://support.apple.com/en-us/HT204904

FIPS 140-2 Validated Algorithms

The **Secure Enclave Processor Secure Key Store (SKS) Cryptographic Module, v1.0** is a hardware cryptographic module offering secure key store services from within the boundary of the embedded Secure Enclave Processor (SEP) to the underlying Apple SoC and its corresponding platform OS. Algorithms from the hardware cryptographic module achieved **Cryptographic Algorithm Validation** under the Cryptographic Algorithm Validation Program (CAVP).

Modes of Operation

The **Secure Key Store (SKS) Module** has FIPS Approved and Non-Approved modes of operation. The module is configured in the system by default and cannot be changed. If the device boots up successfully then the module has passed all self-tests and are operating in the Approved mode.

The Approved security functions are listed in **Table 3: Approved or Allowed Security Functions** of the Non-Proprietary Security Policy documents posted along with the module validation certificate under CMVP. The Security Policy document links can be found above in the *Developer Resources* section. Column four (Val. No.) lists the validation numbers obtained from NIST for successful validation testing of the implementation of the cryptographic algorithms on the platforms as shown in Table 2 under CAVP.

Any calls to the non-Approved security functions listed in **Table 4: Non-Approved Security Functions** of the Non-Proprietary Security Policy documents will cause the module to assume the non-Approved mode of operation.

Note in the Security Policy documents under Key / CSP Establishment that the module provides key transport through SP800-38F AES key wrapping. The module provides key establishment services in the Approved mode through the PBKDF2 algorithm. The PBKDF2 function is provided as a service and returns the key derived from the provided password to the caller. The caller shall observe all requirements and should consider all recommendations specified in SP800-132 with respect to the strength of the generated key, including the quality of the password, the quality of the salt as well as the number of iterations. The implementation of the PBKDF2 function requires the user to provide this information.

Refer to https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program for the current standards, test requirements, and special abbreviations used.

To see the exhaustive list of all algorithms supported by the cryptographic modules, Crypto Officers are highly encouraged to obtain and read the Security Policy document for complete technical explanations on the Secure Enclave Processor Secure Key Store (SKS) Cryptographic Module. Links are provided in the Developer and Crypto Officer Resources section above.

Suite B Cryptographic Algorithms

The Secure Enclave Processor Secure Key Store (SKS) Cryptographic Module does provide for the use of Suite B Cryptographic Algorithms as are called out by NSA. Those algorithms include AES (FIPS 197), ECDH (SP 800-56A), ECDSA (FIPS 186-4) and SHA-256/-384 (FIPS 180-4).

Public Review of Cryptographic Libraries

The same software libraries that secure all Apple Operating Systems are available to third-party developers to help them build advanced security features on Apple platforms.

Cryptographic Libraries **https://developer.apple.com/cryptography/**

— Security Framework

Security Framework provides interfaces for managing certificates, public and private keys, and trust policies. It supports the generation of cryptographically secure pseudorandom numbers. It also supports the storage of certificates and cryptographic keys in the keychain, which is a secure repository for sensitive user data.

— Common Crypto

The Common Crypto library provides additional support for operations like symmetric encryption, hash-based message authentication codes, and digests.

— corecrypto

Although the CoreCrypto Modules do not directly provide programming interfaces for developers and should not be used by iOS, tvOS, watchOS or macOS apps, the source code has been posted and is available to allow for verification of its security characteristics and correct functioning.