Crypto Officer Role Guide for FIPS 140-2 Compliance

for ARM

(iOS 11, tvOS 11, watchOS 4, and T2 Firmware)

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 two Apple Cryptographic Modules achieved **FIPS 140-2 Level 1 Conformance Validation** under the Cryptographic Module Validation Program (CMVP) – a joint American and Canadian security accreditation program for cryptographic modules.

These two modules are identified under the CMVP with the module names of: a) "**Apple CoreCrypto Module v8 for ARM"** and b) "**Apple CoreCrypto Kernel Module v8 for ARM**." The **CoreCrypto Module** is available to developers for Applications and Services running in User Space. The **CoreCrypto Kernel Module** is used only by the Kernel running on ARM processors.

Apple CoreCrypto Module v8 for ARM Validation Certificate #**3148**

csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3148

Apple CoreCrypto Kernel Module v8 for ARM Validation Certificate #**3147**

csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3147

NOTE: Within this and other Apple documents, those modules may also be referred to with the name of **"Apple FIPS Cryptographic Module v8 for ARM"**

Validation References and Resources

CMVP

All Apple Validated Crypto Modules can be found under CMVP's new FIPS 140-2 Validated Cryptographic Module Search page here - https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search. Search for Vendor: "Apple"

Apple

Apple Validated Crypto Modules, related Crypto Officer Role Guides, and links to the Security Policy document and CMVP issued certificates can be found in the Knowledge Base Articles -

Product security certifications, validations, and guidance for …

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 Applications and 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. A cryptographic module may contain additional algorithms that are not FIPS-Approved and if used, would indicate a temporary Non-FIPS Compliant condition. A FIPS 140-2 Level 1 Conformance Validation does not require the cryptographic module restricts applications and services only to use FIPS-Approved algorithms.

Apple

A high-level, non-exhaustive list of Apple applications and services that are FIPS 140-2 Compliant would include the following:

Services

Bluetooth, Data Protection, Hardware Encryption, HTTPS, Keychain Services, S/MIME, TLS/SSL, VPN, and 802.1X.

Applications

App Store, iTunes Store, Calendar, Contacts, FaceTime, Messages, Mail, Safari, and Software Update.

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.

Apple CoreCrypto Module v8.0 for ARM : FIPS 140-2 Non-Proprietary Security Policy
csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3148.pdf

Apple CoreCrypto Kernel Module v8.0 for ARM : FIPS 140-2 Non-Proprietary Security Policy
csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3147.pdf

This Crypto Officer Role Guide 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 on the previous page.

iOS Security Guide

The iOS Security Guide target audience is enterprise IT and provides both an overview and low-level details about the security services, processes and cryptographic algorithms in use throughout various parts of the platform. The iOS Security Guide covers iOS, tvOS and watchOS.

https://www.apple.com/business/docs/iOS_Security_Guide.pdf

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

Certificate, Key, and Trust Services Programming Guide
https://developer.apple.com/library/ios/documentation/Security/Conceptual/CertKeyTrustProgGuide/

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

Storing Keys in the Secure Enclave
https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave

Compliant Platforms

Compliant platforms are the following Apple systems with an A7 - A11 Bionic SoC , S1P and S3 SoC, and the T2 SoC. During the validation process for FIPS 140-2 Conformance, the cryptographic modules are put through operational testing environments on all the evaluated platforms and noted on the issued certificate. The **CoreCrypto** and **CoreCrypto Kernel** modules were validated under the following operational testing environments:

Module: **Apple CoreCrypto Module v8.0 for ARM**

Platforms: **iOS 11** (User Space)

- A7, A8, A8X, A9, A9X, A10 Fusion, A10X Fusion, A11 Bionic

tvOS 11 (User Space)

- A10X Fusion

watchOS 4 (User Space)

- S1P, and S3

T2 Firmware (User Space)

- T2 (iBridge 2,1) (2017 iMac Pro)

Module: **Apple CoreCrypto Kernel Module v8.0 for ARM**

Platforms: **iOS 11** (Kernel Space)

- A7, A8, A8X, A9, A9X, A10 Fusion, A10X Fusion, A11 Bionic

tvOS 11 (Kernel Space)

- A10X Fusion

watchOS 4 (Kernel Space)

- S1P, and S3

T2 Firmware (Kernel Space)

- T2 (iBridge 2,1) (2017 iMac Pro)

Compliant Hardware

For FIPS 140-2 Compliance, the platforms noted above articulate Apple systems which were used for operational testing of the cryptographic modules. The CoreCrypto and CoreCrypto Kernel modules on Apple systems also take advantage of the additional processor embedded cryptographic engine. Compliant hardware are Apple systems meeting the technical specifications to run iOS 11, tvOS 11, watchOS 4, and T2 Firmware.

The platforms validated for **FIPS 140-2 compliance** are listed below and are a subset of all compatible devices as of **March 2018** listed at the corresponding links:

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 Firmware	**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, since iOS 6, have been using the two validated cryptographic modules and performing the required kernel module and algorithm tests. The same statement is now true for tvOS 11, watchOS 4, and T2 Firmware.

These systems will perform all required tests such as the Power-On-Self-Tests (POST) for both the kernel and user space modules, 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 iOS system is physically Powered on

2. Operating System begins the bootstrap process

3. Operating System ensures integrity of the **CoreCrypto Kernel Module**

    3.1. Validation of the `corecrypto.kext`
        3.1.1. The kernel determines operating environment (i.e arm64)
        3.1.2. The kernel reads a validated HMAC_SHA256 from the `corecrypto.kext`
        3.1.3. The `corecrypto.kext` is launched and given the correct validated HMAC from 3.1.2
        3.1.4. The `corecrypto.kext` will generate an HMAC_SHA256 of the corecrypto.kext 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 `corecrypto.kext` performs POST on algorithms and modes
        3.2.2. If any part of the POST fails, the system will panic and halt

4. Operating System ensures Integrity of **CoreCrypto Module**

    4.1. Validation of the `corecrypto.dylib`
        4.1.1. Upon user space environment setup by the kernel, **launchCtl** will launch the integrity test application `/usr/libexec/cc_fips_test`
        4.1.2. The system reads a validated HMAC_SHA256 from the `corecrypto.dylib`
        4.1.3. An HMAC_SHA256 of the user space corecrypto.dylib will be generated and compared to the HMAC_SHA256 value from 4.1.2
        4.1.4. If the calculated HMAC_SHA256 does not match the stored HMAC_SHA256, the system will panic and halt
    4.2. The cipher Power-On-Self-Test (POST) validates the algorithms and modes
        4.2.1. The `cc_fips_test` performs POST on algorithms and modes
        4.2.2. If any part of the POST fails, the system will panic and halt

5. Halt upon failure of any tests

    5.1. 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 modules

A boot-up of the device always forces the FIPS POST which verifies the integrity of both the CoreCrypto Kernel and CoreCrypto modules. If the device boots-up successfully, both modules have passed integrity verification. 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 integrity verification of both cryptographic modules.

How to mitigate integrity issues of the modules

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, 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
- **Resolve iOS update and restore errors in iTunes**

  https://support.apple.com/en-us/HT201210

If needing to perform an Apple Support-wide search for all articles pertaining to "Restoring iOS Software", use the following URL:
http://support.apple.com/kb/index?page=search&product=&q=Restoring%20iOS%20Software&src=support_site.kbase.search.searchresults

If choosing to perform an Apple Support-wide search for all articles pertaining to "FIPS iOS", use the following URL:
http://support.apple.com/kb/index?page=search&product=&q=FIPS%20iOS&src=support_site.kbase.search.searchresults

FIPS 140-2 Validated Algorithms

The CoreCrypto and CoreCrypto Kernel Modules are cryptographic libraries offering various cryptographic mechanisms to Apple frameworks. Algorithms from the two Apple cryptographic modules achieved **Cryptographic Algorithm Validation** under the Cryptographic Algorithm Validation Program (CAVP).

Modes of Operation

The CoreCrypto and CoreCrypto Kernel Modules have an Approved and Non-Approved modes of operation. The Approved mode of operation is configured in the system by default and cannot be changed. If the device boots up successfully then CoreCrypto framework and CoreCrypto KEXT have passed all self-tests and are operating in the Approved mode.

The Approved security functions are listed in **Table 3: Approved or Vendor Affirmed 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. Operators of the modules are strongly advised to avoid calling the functions in Table 4. If the module is operating in the non-Approved mode, operators are strongly cautioned to not use any CSP's previously utilized in the Approved mode of operation.

Note in the Security Policy documents under Key / CSP Establishment that the module provides AES key wrapping, RSA key wrapping, Diffie-Hellman- and EC Diffie-Hellman-based key establishment services in the Approved mode. The module provides key establishment services in the Approved mode through the PBKDFv2 algorithm. The PBKDFv2 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 PBKDFv2 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 CoreCrypto and CoreCrypto Kernel modules. Links are provided in the Developer and Crypto Officer Resources section above.

Suite B Cryptographic Algorithms

The CoreCrypto Module (User Space) 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 libraries that secure all Apple Operating Systems are available to third-party developers to help them build advanced security features.

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.