Apple Inc.

Apple iPad and iPhone Mobile Devices with iOS 11.2

PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0

Common Criteria Guide

Version 2.0
2018-07-12
VID: 10851

Prepared for:
Apple Inc.
One Apple Park Way
MS 927-1CPS
Cupertino, CA 95014
www.apple.com

Prepared by:
atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

Table of Figures

Table of Tables

Revision History

Version	Date	Change
1.0	2018-02-26	Initial Version
1.01	2018-03-30	Changes in response to validators comments
2.0	2018-07-12	Added new equivalent models

1 Introduction

According to the “Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target” ([ST]), the Target of Evaluation (TOE) is a series of Apple iPad and iPhone mobile devices running the iOS 11.2 operating system. The operating system manages the device hardware, provides mobile device agent functionality, and provides the technologies required to implement native applications (apps). iOS 11.2 provides a built-in mobile device management (MDM) application programming interface (API), giving management features that may be utilized by external MDM solutions and allowing enterprises to use profiles to control some of the device settings. The TOE provides a consistent set of capabilities allowing the supervision of enrolled devices. These capabilities include the preparation of devices for deployment, the subsequent management of the devices, and the termination of management.

The TOE does not include the user apps that run on top of the operating system but does include controls that limit application behavior. The TOE is expected but not required to be part of an MDM solution that enables the enterprise to control and administer all TOE instances that are part of the enterprise MDM solution.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the:

- [PP_MD_V3.1] U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals, Version 3.1 (https://www.niap-ccevs.org/Profile/Info.cfm?id=417);
- [EP_MDM_AGENT_V3.0] U.S. Government Approved Protection Profile - Extended Package for Mobile Device Management Agents Version 3.0 (https://www.niap-ccevs.org/Profile/Info.cfm?id=403); and
- [PP_WLAN_CLI_EP_V1.0] Extended Package for WLAN Client Version 1.0 (https://www.niap-ccevs.org/Profile/Info.cfm?id=386)

in the evaluated configuration according to the Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target.

This document provides clarifications and changes to the Apple documentation and shall be used as the guiding document for the configuration and administration of the TOE in the Common Criteria (CC) evaluated configuration. The official Apple documentation should be referred to and followed only as directed within this guiding document. Table *1*: TOE Guidance Documents, lists the guidance documents relevant to the configuration and operation of the TOE.

Document Name	Location
User Guidance	
[iPhone_UG] iPhone User Guide for iOS 11 (2017)	https://help.apple.com/iphone/11/
[iPad_UG] iPad User Guide for iOS 11 (2017)	https://help.apple.com/ipad/11/
Administrator Guidance	

Document Name	Location
[CC_GUIDE] Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Common Criteria Guide	(This document.) https://www.niap-ccevs.org/st/st_vid10851-agd.pdf
Supporting Documents	
[iOSDeployRef] iOS Deployment Reference (V3.9)	https://itunes.apple.com/us/book/ios-deployment-reference/id917468024?mt=11
[OTA_Guide] Over-The-Air Profile Delivery and Configuration Guide (Updated 2018-01-24)	https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html
[IOS_CFG] Configuration Profile Reference (Updated 2018-01-24)	https://developer.apple.com/enterprise/ConfigurationProfileReference.pdf
[AConfig] Apple Configurator 2 Help (online guidance)	http://help.apple.com/configurator/mac/2.6//
[DEP_Guide] Apple Deployment Programs Device Enrollment Program Guide	https://www.apple.com/business/docs/DEP_Guide.pdf
[PM_Help] Profile Manager Help	https://help.apple.com/profilemanager/mac/5.4/
[IOS_LOGS] Profiles and Logs	https://developer.apple.com/bug-reporting/profiles-and-logs/?platforms=ios
[PASSCODE-Help] Use a passcode with your iPhone, iPad or iPod touch	https://support.apple.com/en-us/HT204060
App Developer Guidance	
[3CC-MAN] Common Crypto man pages	https://developer.apple.com/legacy/library/documentation/Darwin/Reference/ManPages/#
[CKTSREF] Certificate, Key, and Trust Services	https://developer.apple.com/documentation/security/certificate_key_and_trust_services
[CRYPTOGUIDE] Cryptographic Services Guide	https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html
[iOS_MDM] Mobile Device Management Protocol Reference	https://developer.apple.com/library/content/documentation/Miscellaneous/Reference/MobileDeviceManagementProtocolRef/1-Introduction/Introduction.html

Document Name	Location
[IPLKEYREF] Information Property List Key Reference	https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Introduction/Introduction.html
[KEYCHAINPG] Keychain Services Programming Guide	https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/01introduction/introduction.html
[SECFWREF] Secure Framework	https://developer.apple.com/library/prerelease/ios/documentation/Security/Reference/SecurityFrameworkReference/index.html
[HTTPSTN2232] Technical Note TN 2232: HTTPS Server Trust Evaluation	https://developer.apple.com/library/ios/technotes/tn2232/_index.html

Table 1: TOE Guidance Documents

1.2 Evaluated TOE Configuration

Table *2*: Devices Covered by the Evaluation, lists the iPhone and iPad devices that are covered by the CC evaluation.

Device Name	Model Number	Processor
iPhone 5s	A1533 (GSM) A1533 (CDMA) A1453 A1457 A1530	A7
iPhone 6 Plus/ iPhone 6	A1549/A1522 (GSM) A1549/A1522 (CDMA) A1586/A1524	A8
iPhone 6s Plus iPhone 6s	A1634/A1633 (US) A1687/A1688 (Global)	A9
iPhone 7 Plus/ iPhone 7	A1784/A1778 (GSM) A1661/A1660 (CDMA)	A10 Fusion
iPhone 8 Plus iPhone 8	A1864/A1898/A1899/A1897 A1863/A1906/A1907/A1905	A11 Bionic
iPhone X	A1865/A1902 A1901	A11 Bionic
iPhone SE	A1662 (US) A1723 (Global)	A9
iPad mini 3	A1599 (Wi-Fi only) A1600 (Wi-Fi + cellular) A1601 (Wi-Fi + cellular)	A7
iPad mini 4	A1538 (Wi-Fi only) A1550 (Wi-Fi + cellular)	A8
iPad Air 2	A1566 (Wi-Fi only) A1567 (Wi-Fi + cellular)	A8X
iPad Pro 12.9”	A1584 (Wi-Fi only) A1652 (Wi-Fi + cellular)	A9X
iPad Pro 9.7”	A1673 (Wi-Fi only) A1674 (Wi-Fi + cellular) A1675 (Wi-Fi + cellular)	A9X

Device Name	Model Number	Processor
iPad	A1822 (Wi-Fi only) A1823 (Wi-Fi + cellular)	A9
iPad 9.7”	A1893 (Wi-Fi only) A1954 (Wi-Fi + cellular)	A10 Fusion
iPad Pro 12.9”	A1670 (Wi-Fi) A1671 (Wi-Fi + cellular)	A10X Fusion
iPad Pro 10.5”	A1701 (Wi-Fi) A1709 (Wi-Fi + cellular)	A10X Fusion

Table 2: Devices Covered by the Evaluation

1.3 Assumptions

The following assumptions apply when operating the TOE in the evaluated configuration. These assumptions must be complied with by the organization through the implementation of appropriate organizational policies and procedures.

1.3.1 [PP_MD_V3.1] Assumptions

- TOE administrators will configure the mobile device's security functions correctly to create the intended security policy.
- The mobile device user will immediately notify the administrator if the mobile device is lost or stolen.
- The mobile device user exercises precautions to reduce the risk of loss or theft of the mobile device.

1.3.2 [PP_WLAN_CLI_EP_V1.0] Assumptions

- Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

1.3.3 [EP_MDM_AGENT_V3.0] Assumptions

- The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
- The MDM Agent relies upon mobile platform and hardware evaluated against the [PP_MD_V3.1] and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM agent.
- One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
- Mobile device users are not willfully negligent or hostile and use the device within compliance of a reasonable Enterprise security policy.

1.4 TOE Security Functionality (TSF)

In the evaluated configuration, the TOE provides the following security functionality required by [PP_MD_V3.1], [EP_MDM_AGENT_V3.0], and [PP_WLAN_CLI_EP_V1.0].

- Security Audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TOE Security Functionality (TSF)
- TOE access
- Trusted path/channels

2 Secure Installation and Delivery

2.1 Secure Installation and Delivery of the TOE

The evaluated devices (TOE devices) are intended for end users who are employees of entities such as business organizations and government agencies.

The administrator of the customer entity is responsible for performing the necessary configuration to ensure that the TOE devices are placed in a configuration specified by the Security Target (ST).

The guidance documentation referenced in this CC Guide for the TOE devices can be accessed and downloaded from the Apple website as given in Table *1*: TOE Guidance Documents.

The normal distribution channels for obtaining these devices include the following:

- The Apple Store (either a physical store or online at https://apple.com)
- Apple retailers
- Service carriers (e.g., AT&T, Verizon)
- Resellers

Business

There is a distinct online store for Business customers with a link from the “Apple Store.” From the link to the “Apple Store” (https://www.apple.com), go to the upper left of the page and click “Business Store Home.” Or, optionally, use the following link.

https://www.apple.com/us_smb_78313/shop

Government

Government customers can use the following link.

https://www.apple.com/r/store/government/

Additional

Large customers can also have their own Apple Store Catalog for their employees to purchase devices directly from Apple under their corporate employee purchase program.

2.2 Secure Software Updates

All iOS updates are digitally signed. The user can verify the software version of the TOE on the devices. Refer to section 3.7, *Obtain Version Information*, for more information.

Software updates to the TOE are released regularly to address emerging security concerns and also provide new features; these updates are provided for all supported devices simultaneously. Users receive iOS update notifications on the device and through iTunes. Updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes.

The device startup process helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS uses a process called System Software Authorization. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS and exploit a vulnerability that has been fixed in the newer version.

On a device with an A7 or later A-series system on a chip (SoC) the Secure Enclave processor (SEP) also utilizes System Software Authorization to ensure the integrity of its software and prevent downgrade installations.

iOS software updates can be installed using iTunes or over-the-air (OTA) on the device. With iTunes, a full copy of iOS is downloaded and installed. OTA software updates download only the components required to complete an update, rather than downloading the entire OS, improving network efficiency. Additionally, software updates can be cached on a local network server running the caching service on OS X Server so that iOS devices do not need to access Apple servers to obtain the necessary update data.

During an iOS upgrade, iTunes (or the device itself, in the case of OTA software updates) connects to the Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, low-level bootloader (LLB), iBoot, the kernel, and OS image), a random anti-replay value (nonce), and the device's unique Electronic Chip ID (ECID).

The authorization server checks the presented list of measurements against versions for which installation is permitted and, if it finds a match, adds the ECID to the measurement and signs the result. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID "personalizes" the authorization for the requesting device. By authorizing and signing only for known measurements, the server ensures that the update takes place exactly as provided by Apple.

The boot-time chain-of-trust evaluation verifies that the signature comes from Apple and that the measurement of the item loaded from disk, combined with the device's ECID, matches what was covered by the signature.

These mechanisms ensure that the authorization is for a specific device and that an old iOS version from one device cannot be copied to another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software.

Note that this ensures the integrity and authenticity of software updates. A TLS trusted channel is provided for this process.

2.3 Unevaluated Functionalities

The following security functionalities were not evaluated as part of the iOS 11.2 TOE and considered outside the scope of the evaluation.

2.3.1 Two-Factor Authentication

According to the [iPad_UG] and the [iPhone_UG] Privacy and security, Security, Two-factor authentication, Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password. It's built into iOS 9 and later, and OS X 10.11 and later.

This feature is outside the scope of the evaluated configuration.

2.3.2 Bonjour

According to the [iOSDeployRef], Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network.

This feature is outside the scope of the evaluated configuration.

2.3.3 Unsupported VPN Protocols and Authentication Methods

The use of the following Virtual Private Network (VPN) protocols (and their authentication methods) which are described in the [iOSDeployRef] are outside the scope of the evaluated configuration.

- Cisco IPSec

- Layer Two Tunneling Protocol (L2TP) over IPSec
- Point-to-Point Tunneling Protocol (PPTP)

In addition, the following authentication methods are unsupported.

- L2TP over IPSec: user authentication by Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) password, two-factor token, machine authentication by shared secret
- Cisco IPSec: user authentication by password, two-factor token, machine authentication by shared secret and certificates
- PPTP: user authentication by MS-CHAP v2 password, two-factor token
- Secure Sockets Layer (SSL) VPN: user authentication by password, two-factor token, certificates

2.3.4 VPN Split Tunnel

VPN split tunnel as described in the [iOSDeployRef] is outside of the evaluated configuration.

2.3.5 Siri Interface

The Siri interface as described in the [iPad_UG] and [iPhone_UG]

Since the Siri interface supports some commands related to configuration settings (For example, switching WiFi and Bluetooth on and off) the Siri interface must be turned off.

To turn Hey Siri on or off, go to *Settings»Siri & Search»Listen for "Hey Siri"*.

Siri can also be disabled using a configuration profile setting as described in Section 3.1, *Configuration Profiles*.

