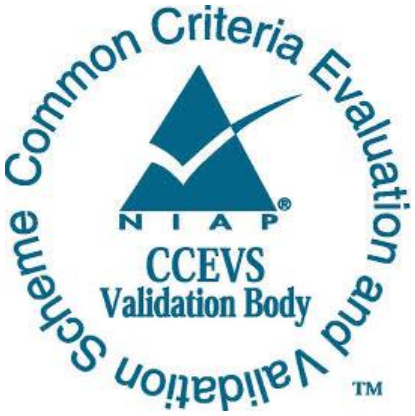
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Apple iPad and iPhone Mobile Devices with iOS 12

Report Number: CCEVS-VR-10937-2019

Dated: March 14, 2019

Version: 0.2

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Sheldon A. Durrant

Michelle S. Carlson

John Butterworth

MITRE Corporation

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Trang Huynh
King Ables
Quentin Gouchet
Stephan Mueller

atsec information security corporation

Austin, TX

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of iPad and iPhone devices with Apple iOS 12 provided by Apple Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in March, 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Extended, and meets the assurance requirements given in:

- The Mobile Device Fundamentals Protection Profile Version 3.1, [PP_MD_V3.1];
    - The Extended Package for Mobile Device Management Agents Version 3.0 [EP_MDM_AGENT_V3.0];
    - The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network {WLAN} Clients, Version 1.0, [PP_WLAN_CLI_EP_V1.0]; and
    - The PP-Module for Virtual Private Network [VPN] Clients, Version 2.1, [MOD_VPN_CLI_V2.1].

The TOE is Apple iPad and iPhone Mobile Devices with iOS 12 executing on the following platforms:

- iPhone 6 Plus / iPhone 6 (A8 processor)
- iPhone 6s Plus / iPhone 6s (A9 processor)

- iPhone 7 / iPhone 7 Plus (A10 Fusion processor)
- iPhone 8 / iPhone 8 Plus (A11 Bionic processor)
- iPhone X (A11 Bionic processor)
- iPhone XS (A12 Bionic processor)
- iPhone XS Max (A12 Bionic processor)
- iPhone XR (A12 Bionic processor)
- iPhone SE (A9 processor)
- iPad mini 4 (A8 processor)
- iPad Air 2 (A8X processor)
- iPad 9.7-inch (A9 processor)
- iPad 9.7-inch (A10 Fusion procession)
- iPad Pro 9.7-inch (A9X processor)
- iPad Pro 12.9-inch (A9X processor)
- iPad Pro 12.9-inch (A10X Fusion processor)
- iPad Pro 10.5-inch (A10X Fusion processor)
- iPad Pro 11-inch (A12X Bionic processor)
- iPad Pro 12.9-inch (A12X Bionic processor)

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC) and the Assurance Activities (AA) of the aforementioned Protection Profile, Extended Packages, and PP Module. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, reviewed testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The CCTL atsec information security corporation evaluation team concluded that the CC requirements specified by:

- The Mobile Device Fundamentals Protection Profile Version 3.1, [PP_MD_V3.1];
    - The Extended Package for Mobile Device Management Agents Version 3.0 [EP_MDM_AGENT_V3.0];
    - The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network {WLAN} Clients, Version 1.0, [PP_WLAN_CLI_EP_V1.0]; and
    - The PP-Module for Virtual Private Network [VPN] Clients, Version 2.1, [MOD_VPN_CLI_V2.1].

have been met.

The technical information included in this report was obtained from the Validation Report for Apple iPad and iPhone Devices with iOS 12 Security Target (ST) Version 1.6 and analysis performed by the Validation Team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

The following table provides information needed to completely identify the product, including the following.

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST): describing the security features, claims, and assurances of the product
- The conformance results of the evaluation
- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme

Item	Identifier
TOE	Apple iPad and iPhone Mobile Devices with iOS 12 executing on the following platforms: • iPhone 6 Plus / iPhone 6 (A8 processor) • iPhone 6s Plus / iPhone 6s (A9 processor) • iPhone 7 / iPhone 7 Plus (A10 Fusion processor) • iPhone 8 / iPhone 8 Plus (A11 Bionic processor) • iPhone X (A11 Bionic processor) • iPhone XS (A12 Bionic processor) • iPhone XS Max (A12 Bionic processor) • iPhone XR (A12 Bionic processor) • iPhone SE (A9 processor) • iPad mini 4 (A8 processor) • iPad Air 2 (A8X processor) • iPad 9.7-inch (A9 processor) • iPad 9.7-inch (A10 Fusion processor) • iPad Pro 9.7-inch (A9X processor) • iPad Pro 12.9-inch (A9X processor) • iPad Pro 12.9-inch (A10X Fusion processor) • iPad Pro 10.5-inch (A10X Fusion processor) • iPad Pro 11-inch (A12X Bionic processor) • iPad Pro 12.9-inch (A12X Bionic processor)
PP	• Protection Profile for Mobile Device Fundamentals Version 3.1, 16 June 2017 • Extended Package for Mobile Device Management Agents Version 3.0, 21 November 2016 • General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, dated 8 February, 2016 • PP-Module for Virtual Private Network {VPN} Clients, Version 2.1, dated 5 October, 2017.
ST	Apple iPad and iPhone Mobile Devices with iOS 12 Security Target (ST) Version 1.6, dated 2019-03-12
ETR	Evaluation Technical Report for a Target of Evaluation Apple iPad and iPhone Mobile Devices with iOS 12
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5

Item	Identifier
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Apple Inc.
Developer	Apple Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Sheldon A. Durrant, Michelle S. Carlson, John Butterworth, MITRE Corporation Kenneth Stutterheim, The Aerospace Corporation

3. Architectural Information

Note that the following architectural description is based on the description presented in the ST.

The implementation of TOE architecture can be viewed as a set of layers. Lower layers contain fundamental services and technologies. Higher-level layers build upon the lower layers and provide more sophisticated services and technologies.

These individual layers provide the following services.

The **Cocoa Touch layer** contains key frameworks for building iOS apps. These frameworks define the appearance of applications (apps).

The **Media layer** contains the graphics, audio, and video technologies you use to implement multimedia experiences in apps.

The **Core Services layer** contains fundamental system services for apps. Key among these services are the Core Foundation and Foundation frameworks, which define the basic types that all apps use. This layer also contains individual technologies to support features such as location, iCloud, social media, and networking. This layer also implements data protection functions that allow apps that work with sensitive user data to take advantage of the built-in encryption available on some devices.

The **Core OS layer** contains the low-level features that most other technologies are built upon. Situations where an app needs to explicitly deal with security or communications with an external hardware accessory, it does so by using the frameworks in this layer.

Security related frameworks provided by this layer are as follows.

- The Generic Security Services Framework, which provides services as specified in RFC 2743 (Generic Security Service Application Program Interface Version 2, Update 1) and RFC 4401 (Pseudo Random Function);
- The Local Authentication Framework;
- The Network Extension Framework, which provides support for configuring and controlling virtual private network (VPN) tunnels;
- The Security Framework, which provides services to manage and store certificates, public and private keys, and trust policies. This framework also provides the Common

Crypto library for symmetric encryption and hash-based message authentication codes and

- The System Framework, which provides the kernel environment, drivers, and low-level UNIX interfaces. The kernel manages the virtual memory system, threads, file system, network, and inter-process communication and is therefore responsible for separating apps from each other and controlling the use of low-level resources.

The TOE may be managed by an MDM solution that enables an enterprise to control and administer the TOE instances that are enrolled in the MDM solution.

TOE Evaluated Configuration

The evaluation covers following Apple iPad and iPhone mobile devices running iOS 12 operating system as detailed in Table 1, below.

Table 1: Devices covered by the evaluation

Processor	Device Name	Model Number
A8	iPhone 6	A1549
		A1586
		A1589
	iPhone 6 Plus	A1522
		A1524
		A1593
	iPad mini 4	A1538
		A1550
A8X	iPad Air 2	A1566
		A1567
A9	iPhone 6s	A1633
		A1688
		A1691
		A1700
	iPhone 6s Plus	A1634
		A1687
		A1690
		A1699
		A1700
	iPhone SE	A1662
		A1723

Processor	Device Name	Model Number
		A1724
	iPad 9.7-inch (5th generation)	A1822
		A1823
A9X	iPad Pro 12.9-inch	A1584
		A1652
	iPad Pro 9.7-inch	A1673
		A1674
		A1675
A10 Fusion	iPhone 7	A1660
		A1779
		A1780
		A1778
	iPhone 7 Plus	A1661
		A1785
		A1786
		A1784
	iPad 9.7-inch (6th generation)	A1893
		A1954
A10X Fusion	iPad Pro 12.9-inch (2nd generation)	A1670
		A1671
		A1821 (China)
	iPad Pro 10.5-inch	A1701
		A1852
		A1709
A11 Bionic	iPhone 8	A1863
		A1906
		A1907
		A1905
	iPhone 8 Plus	A1864
		A1898
		A1899
		A1897
	iPhone X	A1865

Processor	Device Name	Model Number
		A1902
		A1901
A12 Bionic	iPhone XS	A1920
		A2097
		A2098
		A2099
		A2100 (China)
	iPhone XS Max	A1921
		A2101
		A2102
		A2103
		A2104 (China)
	iPhone XR	A1984
		A2105
		A2106
		A2107
		A2108 (China)
	iPad Pro 11-inch	A1934
		A1979 (China)
		A1980
		A2013
	iPad Pro 12.9-inch	A2014
		A1876
		A1895
		A1983 (China)

Physical Scope of the TOE

The TOE is a Mobile Device which consists of a hardware platform and its system software. It provides wireless connectivity and includes software for VPN connections to access the protected enterprise network and other Mobile Devices.

The TOE provides secured communication channels between itself and other trusted IT products using IEEE 802.11-2012, IEEE 802.1X, EAP-TLS, TLS, IPsec, Bluetooth, and NFC (iPhone devices only). Via the established network connection, the TOE can communicate with an MDM server allowing administrative control of the TOE.

Un-evaluated Functionality

The following functions were not evaluated and are therefore not included in the secure configuration of the mobile devices.

- **Two-Factor Authentication**

  Two-factor authentication is an extra layer of security for an Apple ID used in the Apple store, iCloud and other Apple services.

- **Bonjour**

  Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network.

- **VPN Split Tunnel**

  VPN split tunnel is not included in the evaluation, and must be disabled in the mobile device configurations to meet the requirements of this CC evaluation.

- **Siri Interface**

  The Siri interface is capable of supporting commands related to configuration settings.

- **Shared iPad for education**

  This multi-user configuration was not included in the evaluation and must not be used to meet the requirements of this CC evaluation.

- **Third-party MDM Agents**

  Third-party applications are available that provide functionality as a mobile device MDM Agent. No third-party MDM Agent applications were included in the evaluation and are outside the scope of the evaluated configuration.

- **VPN Protocols and Authentication Methods**

  The following Virtual Private Network (VPN) protocols are not included in the evaluation and must be disabled in the mobile device configurations that meet the requirements of this CC evaluation.

  - Cisco IPsec
  - Layer Two Tunneling Protocol (L2TP) over IPsec
  - Secure Sockets Layer (SSL) VPN
  - Shared secret authentication

4. Security Policy

This section summaries the security functionality of the TOE including the following.

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Protection of the TSF (TOE Security Functionality)
7. TOE access
8. Trusted Path/Channels
9. Objective Requirements

Security Audit

The TOE provides the ability for responses to be sent from the MDM Device Agent to the MDM Server. These responses are configurable by the organization using a scripting language given in the Over-the-Air Profile Delivery and Configuration document.

Cryptographic Support

The TOE provides cryptographic services for the encryption of data-at rest, secure communication channels, and for use by applications. In addition, the TOE implements several cryptographic protocols that can be used to establish a trusted channel to other IT entities.

As noted in the Security Target, section 1.5.2.1 the TOE provides cryptographic services via the following cryptographic modules.

- Apple CoreCrypto Cryptographic Module for ARM, v9.0 (User Space)
- Apple CoreCrypto Kernel Module for ARM, v9.0 (Kernel Space)
- Apple Secure Key Store Cryptographic Module, v9.0

The **Apple CoreCrypto Cryptographic Module v9.0 for ARM** is for library use within the iOS user space. A second instance of this module is used within the secure enclave to provide cryptographic services there.

The cryptographic functions provided include symmetric key generation, encryption and decryption using the Advanced Encryption Standard (AES) algorithms, asymmetric key generation and key establishment, cryptographic hashing, and keyed-hash message authentication.

The functions listed below are used to implement the security protocols supported and the encryption of data-at-rest.

- Random Number Generation
- Symmetric Key Generation
- Symmetric Encryption and Decryption

- Digital Signature and Asymmetric Key Generation
- Message Digest
- Keyed Hash
- PBKDF
- EC Diffie-Hellman

The **Apple CoreCrypto Kernel Cryptographic Module for ARM, V9.0** is an iOS kernel extension optimized for library use within the iOS kernel.

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.

The cryptographic services provided by the module are:

- data encryption / decryption
- generation of hash values
- key wrapping
- random number generation
- key generation
- key derivation

User Data Protection

User data in files is protected using cryptographic functions, password protection and encryption to ensure data remains protected even if the device is lost or stolen. Critical data like passwords used by applications or application defined cryptographic keys can be stored in the key chain, which provides additional protection. Data can be protected such that only the application that owns the data can access it.

The Secure Enclave Processor (SEP), is a separate CPU that executes a stand-alone operating system and provides protection for critical security data such as keys.

Identification and Authentication

Except for making emergency calls, answering calls, using the cameras and the flashlight, users need to authenticate using a passcode or a biometric (fingerprint or face). Also, upon power up, or after an update of iOS, the user is required to use the passcode authentication mechanism.

The passcode can be configured to meet dedicated passcode policies, a maximum life time and a minimum length. Passcodes are obscured upon entry, and both the frequency of entering passcodes, as well as the number of consecutive failed attempts, is limited.

The TOE enters a locked state after a configurable time of user inactivity and the user is required to either enter their passcode or use biometric authentication to unlock the TOE.

External entities connecting to the TOE via a secure protocol (Extensible Authentication Protocol Transport Layer Security (EAP-TLS), Transport Layer Security (TLS), IPsec) can be authenticated using X.509 certificates.

Security Management

Security functions can be managed either by the user or by an authorized administrator through a Mobile Device Management system. Table 4 of the Security Target identifies the functions that can be managed and if the management function can be performed by the user, the authorized administrator or both.

Protection of the TSF

Some of the functions the TOE implements to protect the TSF and TSF data are as follows.

- Protection of cryptographic keys
- Use of memory protection and processor states to separate applications and protect the TSF from unauthorized access to TSF resources
- Digital signature protection of the TSF image
- Software/firmware integrity self-test upon start-up
- Digital signature verification for applications
- Access to defined TSF data and TSF services only when the TOE is unlocked

TOE Access

The TSF provides functions to lock the TOE upon request and after an administrator-configurable time of inactivity.

Access to the TOE via a wireless network is controlled by user/administrator defined policy.

Trusted Path/Channels

The TOE supports the use of the following cryptographic protocols that define a trusted channel between itself and another trusted IT product.

- IEEE 802.11-2012
- IEEE 802.1X
- EAP-TLS (1.0, 1.1, 1.2)
- TLS (1.2)
- IPsec
- Bluetooth (4.0, 4.2, 5.0)

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in

- The Mobile Device Fundamentals Protection Profile Version 3.1, [PP_MD_V3.1];
    - The Extended Package for Mobile Device Management Agents Version 3.0 [EP_MDM_AGENT_V3.0];
    - The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network {WLAN} Clients, Version 1.0, [PP_WLAN_CLI_EP_V1.0]; and
    - The PP-Module for Virtual Private Network [VPN] Clients, Version 2.1, [MOD_VPN_CLI_V2.1].

That information has not been reproduced here and the respective documents should be consulted if there is interest in that material. Additionally, the Security Problem Description has been presented in the Security Target.

Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in

- The Mobile Device Fundamentals Protection Profile Version 3.1, [PP_MD_V3.1];
    - The Extended Package for Mobile Device Management Agents Version 3.0 [EP_MDM_AGENT_V3.0];
    - The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network {WLAN} Clients, Version 1.0, [PP_WLAN_CLI_EP_V1.0]; and
    - The PP-Module for Virtual Private Network [VPN] Clients, Version 2.1, [MOD_VPN_CLI_V2.1]

as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note: As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0 and PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1) performed by the evaluation team.

6. Documentation

The following documentation was used as evidence for the evaluation of the TOE.

Design Documentation

None

Guidance Documentation

The following documentation was used as evidence for the evaluation.

Reference	Document Name	Location
Device Administrator Guidance		
[CC_GUIDE]	Apple iPad and iPhone Mobile Devices with iOS 12 Common Criteria Configuration Guide	https://www.niap-ccevs.org/st/st_vid10937-agd.pdf
[IOS_CFG] (2018-09-17)	Configuration Profile Reference	https://developer.apple.com/enterprise/documentation/Configuration-Profile-Reference.pdf
Device User Guidance		
[iPhone_UG]	iPhone User Guide for iOS	https://help.apple.com/iphone/12/
[iPad_UG]	iPad User Guide for iOS	https://help.apple.com/ipad/12/
[PASSCODE-Help] (June 8, 2018)	Use a passcode with your iPhone, iPad or iPod touch	https://support.apple.com/en-us/HT204060
Mobile Device Management		
[AConfig]	Apple Configurator Help (online guidance)	https://help.apple.com/configurator/mac/
[DEP_Guide] (12-2017)	Apple Deployment Programs Device Enrollment Program Guide	https://www.apple.com/business/docs/DEP_Guide.pdf
[PM_Help] (2018)	Profile Manager Help	https://help.apple.com/profilemanager/mac/
[IOS_MDM] (2018-09-17)	Mobile Device Management Protocol Reference	https://developer.apple.com/enterprise/documentation/MDM-Protocol-Reference.pdf
Supporting Documents		

Reference	Document Name	Location
[iOSDeployRef]	iOS Deployment Reference	https://help.apple.com/deployment/ios/
[IOS_LOGS]	Profiles and Logs	https://developer.apple.com/bug-reporting/profiles-and-logs/?platforms=ios
[LOGGING]	Logging	https://developer.apple.com/documentation/os/logging?language=objc
[MDM_SETTINGS_IT]	Mobile device management settings for IT	https://help.apple.com/deployment/mdm/
[TRUST_STORE]	List of available trusted root certificates in iOS 12, macOS 10.14, watchOS 5, and tvOS 12	https://support.apple.com/en-us/HT209144
[MANAGE_CARDS]	Manage the cards that you use with Apple Pay	https://support.apple.com/en-us/HT205583
[PAY_SETUP]	Set up Apple Pay	https://support.apple.com/en-us/HT204506
App Developer Guidance		
[CKTSREF] (2018)	Certificate, Key, and Trust Services	https://developer.apple.com/documentation/security/certificate_key_and_trust_services
[KEYCHAINPG] (2018)	Keychain Services Programming Guide	https://developer.apple.com/documentation/security/keychain_services
[IOS_SEC] (September 2018)	iOS Security (iOS 12)	https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

Any additional customer documentation delivered with the product or that may be available through download was not included in the scope of the evaluation and hence should not be relied upon when configuring or using the products in the evaluated configuration.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

Evaluation Team Independent Testing

The ST lists more devices compared to the subset of devices used for testing. The tests were performed by choosing one device from within each device family containing the hardware that affects TSF operation: the CPU.

The other hardware configuration items such as form factor, size of non-volatile storage, presence or absence of modem devices, etc. do not affect the TSF, because all TSF functions are solely implemented in software that uses the process isolation and memory separation capabilities offered by the CPU. The software of the TOE is compiled once to form one set of binaries which run unchanged on all devices, and therefore on all CPUs equally. Based on this equivalency consideration, the evaluators used the hardware information provided by the developer, which lists all devices found in the ST and references the CPUs used by those devices. All devices listed in the ST use one of the following CPUs:

- A8
- A8X
- A9
- A9X
- A10 Fusion
- A10X Fusion
- A11 Bionic
- A11X Bionic
- A12 Bionic
- A12X Bionic

The test system was set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing.

The testing was performed by setting up a Linux server that operated as a:

- WLAN access point,
- VPN endpoint,
- VPN Gateway with the Strongswan IKE daemon and the Linux kernel IPsec support
- Web server with TLS support,
- Key generator, and
- Bluetooth endpoint.

The Linux system was equipped with the appropriate tools to perform sniffing of the different traffic types and analyzing the traffic, e.g., wireshark, tcpdump, bluez-hcidump.

Apple Configurator was used to create the configuration profiles/policies and deploy the profiles/policies onto the different test systems. An Apple system hosting the Apple Profile Manager software component acted as the MDM server to which the test devices connected.

8. Evaluated Configuration

The guidance documentation provides specific instructions for creating configuration profiles that configure Apple iOS to comply with the functions defined in the Security Target. The evaluated configuration included the devices listed below running Apple iOS 12:

- Apple device with CPU A8: Apple iPhone 6 Plus, iPhone 6
- Apple device with CPU A8X: Apple iPad Air 2
- Apple device with CPU A9: Apple iPhone 6s, iPhone 6s Plus
- Apple device with CPU A9X: Apple iPad Pro 9.7-inch, iPad Pro 12.9-inch
- Apple device with CPU A10 Fusion: Apple iPhone 7, iPhone 7 Plus
- Apple device with CPU A10X Fusion: Apple iPad Pro 12.9-inch
- Apple device with CPU A11 Bionic: Apple iPhone 8, iPhone 8 Plus, iPhone X
- Apple device with CPU A12 Bionic: Apple iPhone Xs Max, iPhone Xs
- Apple device with CPU A12X Bionic: Apple iPad Pro 11-inch

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

All work units defined by CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements as well as assurance activities. The evaluation was conducted based upon CEM Version 3.1 Revision 5. The evaluation determined the TOE to be CC Part 2 extended and Part 3 extended, and to meet the assurance requirements defined by the PP_MD_V3.1, EP_MDM_AGENT_V3.0 PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1.

Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1. The ST evaluation ensured the ST contains a description of the

environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Apple iOS 12 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and Guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both the administrator and user guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0 and MOD_VPN_CLI_V2.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer can identify the evaluated TOE.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed devised an independent set of tests as mandated by the protection profile.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 and that the conclusion reached by the evaluation team was justified.

Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1, and MOD_VPN_CLI_V2.1. The vendor provided security updates to the TOE during the evaluation, therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates, in line with the guidance provided in Scheme Policy Letter 15, fixed all known issues. The evaluation team ensured that the currently available version of the TOE does not contain known exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The evaluators searched for publicly known vulnerabilities applicable to iOS using the following sources:

- Apple security content disclosure statements for releases of iOS 12 related to this evaluation
- MITRE Common Vulnerabilities and Exposures (CVE) List
- NIST National Vulnerability Database (NVD)

using the following search terms:

- ios ipad
- ios iphone
- ios core tls
- ios core crypto
- ios common crypto

- ios http
- ios https
- ios tcp
- ios ip
- ios bluetooth
- ios ipsec
- ios vpn
- ios mdm
- ios mobile
- broadcom wi-fi

The evaluator's CVE search found no vulnerabilities apart from the ones listed in the developer's security content disclosure statements, all of which have been fixed in subsequent releases of iOS.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 and that the conclusion reached by the evaluation team was justified.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the testing defined by the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0 and MOD_VPN_CLI_V2.1 and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM and the PP_MD_V3.1, EP_MDM_AGENT_V3.0, PP_WLAN_CLI_EP_V1.0, and MOD_VPN_CLI_V2.1 and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

<none>

11. Annexes

Not applicable.

12. Security Target

Apple iPad and iPhone Mobile Devices with iOS 12 Security Target (ST) Version 1.6, dated 2019-03-12

13. Glossary

The following definitions are used throughout this document.

AA	Assurance Activity
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CDMA	Code Division Multiple Access
CCTL	Common Criteria Testing Laboratory—An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
CEM	Common Criteria Evaluation Methodology
CPU	Central Processing Unit
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EC	Elliptic Curve
EP	Extended Package (for a Protection Profile)
ETR	Evaluation Technical Report
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
GSM	Global System for Mobile Communication
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-hash Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange

LTE	Long-Term Evaluation
MDM	Mobile Device Management
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PBKDF	Password Based Key Derivation Function
PP	Protection Profile
REK	Root Encryption Key
RFC	Request For Comments
SEP	Secure Enclave Processor
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation—A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
TLS	Transport Layer Security
TSF	TOE Security Functionality
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
VPN	Virtual Private Network
VR	Validation Report
WLAN	Wireless Local Area Network

14. Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017.

- Extended Package for Mobile Device Management Agents, Version 3.0, 21 November 2016.
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Client, Version 1.0, 08 February 2016
- PP-Module for VPN Client Version 2.1, 05 October 2017
- Apple iPad and iPhone Mobile Devices with iOS 12 Common Criteria Configuration Guide, Version 1.7, 2019-03-12
- Apple iPad and iPhone Mobile Devices with iOS 12 Security Target Version 1.6, 2019-03-12
- Assurance Activity Report, Version 1.1, 2019-03-12