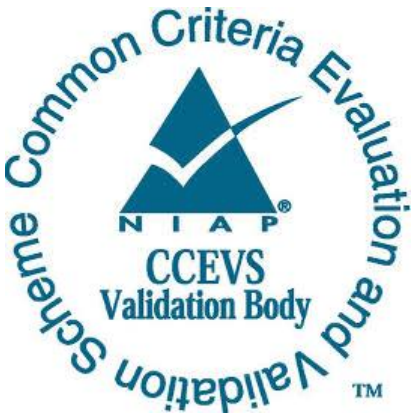
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Apple iOS 10.2

Report Number: CCEVS-VR-10782-2017
Dated: July 27, 2017 Version: 1.0

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

Lead Validator Patrick Mallett, PhD

MITRE Corporation
McLean, VA

Kenneth Stutterheim

The Aerospace Corporation
Columbia, MD

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 the iOS 10.2 solution 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 July, 2017. The information in this report is largely derived from the proprietary 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 set forth in the Mobile Device Fundamentals Protection Profile version 3.0; the Extended Package for Mobile Device Management Agents Version 3.0 and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients Version 1.0.

The TOE is the Apple iOS 10.2 operating system executing on a wide selection of hardware components, as follows.

- iPhone 6 Plus / iPhone 6 (A8 processor)
- iPhone 6s Plus / iPhone 6s (A9 processor)
- iPhone SE
- iPhone 5s
- iPad mini 3
- iPad mini 4
- iPad Air 2
- iPad mini 2
- iPad Air
- iPad Pro 12.9”
- iPad Pro 9.7”
- iPhone 7 / iPhone 7 Plus
- iPad

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 4)” (CEM) for conformance to the “Common Criteria for IT Security Evaluation (Version 3.1, Rev 4)” (CC). 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 of 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 Fundamental Protection Profile" (MDFPP) version 3.0, the Extended Package for Mobile Device Management Agents Version 3.0 (MDMAEP) and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients Version 1.0 (WLANEP) have been met.

The technical information included in this report was obtained from the Apple iOS 10.2 MDFPP v3/ EP MDM AGENTV3.0 / PP WLAN CLI EP V1.0 Security Target (ST) 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 Validated Products List.

Table 1 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 result of the evaluation
- The Protection Profiles to which the product is conformant
- The organizations and individuals participating in the evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iOS 10.2 executing on the following hardware: • iPhone5s • iPhone 6 / iPhone 6 Plus • iPhone 6S / iPhone 6S Plus • iPhone 7 / iPhone 7 Plus • iPhone SE • iPad mini 2 • iPad mini 3 • iPad mini 4 • iPad Air • iPad Air 2 • iPad Pro 12.9” • iPad Pro 9.7” • iPad
PP	Protection Profile for Mobile Device Fundamentals Version 3.0, 10 December 2016 Extended Package for Mobile Device Management Agents Version 3.0, 21 November 2016 Extended Package for Wireless LAN Client Version 1.0, 11 February 2016
ST	Apple iOS 10.2 PP_MD_V3.0, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target, Version 2.0, Date: July 27, 2017
ETR	Evaluation Technical Report for a Target of Evaluation Apple iOS 10.2 with MDM Agent and WLAN CLI
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
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	Patrick Mallet, MITRE Corporation, McLean, VA Kenneth Stutterheim, The Aerospace Corporation, Columbia, MD

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). They also provide the basic app infrastructure and support for key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. When designing apps, one should investigate the technologies in this layer first to see if they meet the needs.

The **Media layer** contains the graphics, audio, and video technologies you use to implement multimedia experiences in apps. The technologies in this layer make it easy to build apps that look and sound great.

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. When an app designates a specific file as protected, the system stores that file on disk in an encrypted format. While the device is locked, the contents of the file are inaccessible to both the app and to any potential intruders. However, when the device is unlocked by the user, a decryption key is created to allow the app to access the file. Other levels of data protection are also available.

The Core OS layer contains the low-level features that most other technologies are built upon. Even if an app does not use these technologies directly, they are most likely being used by other frameworks. And in situations where an app needs to explicitly deal with security or communicating 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.

3.1 TOE Evaluated Configuration

The evaluation covers Apple iOS 10.2 on the following devices as detailed in Tables 2 and 3, below.

Table 2: Devices Covered by the Evaluation

Device Name	Model Number	Proc-essor	WiFi	Cellular	Bluetooth
iPhone 5s	**A1533 (GSM)** **A1533 (CDMA)** **A1453** **A1457** **A1530**	**A7**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**See Table 3** **See Table 3** **See Table 3** **See Table 3** **See Table 3**	**4.0** **4.0** **4.0** **4.0** **4.0**
iPhone 6 Plus/ iPhone 6	**A1549/A1522 (GSM)** **A1549/A1522 (CDMA)** **A1586/A1524**	**A8**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**See Table 3** **See Table 3** **See Table 3**	**4.0** **4.0** **4.0**
iPhone 6S Plus / **iPhone 6S**	**A1634/A1633 (US)** **A1687/A1688 (Global)**	**A9**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**See Table 3** **See Table 3**	**4.2** **4.2**
iPhone 7 Plus/ **iPhone 7**	**A1784/A1778 (GSM)** **A1661/A1660 (CDMA)**	**A10**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**See Table 3** **See Table 3**	**4.2** **4.2**

Device Name	Model Number	Proc-essor	WiFi	Cellular	Bluetooth
iPhone SE	**A1662 (US)** **A1723 (Global)**	**A9**	**802.11/a/b/g/ n/ac**	**See Table 3**	**4.2**
iPad mini 2	**A1489 (WiFi only)** **A1490 (WiFi + cellular)** **A1491 (WiFi + cellular)**	**A7**	**802.11a/b/g/n** **802.11a/b/g/n** **802.11a/b/g/n**	**-** **See Table 3** **See Table 3**	**4.0** **4.0** **4.0**
iPad mini 3	**A1599 (WiFi only)** **A1600 (WiFi + cellular)** **A1601 (WiFi + cellular)**	**A7**	**802.11a/b/g/n** **802.11a/b/g/n** **802.11a/b/g/n**	**-** **See Table 3** **See Table 3**	**4.0** **4.0** **4.0**
iPad mini 4	**A1538 (WiFi only)** **A1550 (WiFi + cellular)**	**A8**	**802.11a/b/g/n** **802.11a/b/g/n**	**-** **See Table 3**	**4.2** **4.2**
iPad Air	**A1474 (WiFi only)** **A1475 (WiFi + cellular)** **A1476 (WiFi + cellular)**	**A7**	**802.11a/b/g/n** **802.11a/b/g/n** **802.11a/b/g/n**	**-** **See Table 3** **See Table 3**	**4.0** **4.0** **4.0**
iPad Air 2	**A1566 (WiFi only)** **A1567 (WiFi + cellular)**	**A8X**	**802.11a/b/g/n /ac** **802.11a/b/g/n /ac**	**-** **See Table 3**	**4.2** **4.2**
iPad Pro 12.9”	**A1584 (WiFi only)** **A1652 (WiFi + cellular)**	**A9X**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**-** **See Table 3**	**4.2** **4.2**
iPad Pro 9.7”	**A1673 (WiFi only)** **A1674 (WiFi + cellular)**	**A9X**	**802.11/a/b/g/ n/ac** **802.11/a/b/g/ n/ac**	**-** **See Table 3**	**4.2** **4.2**
iPad	**A1822 (WiFi only)**	**A9**	**802.11/a/b/g/ n/ac**	**-**	**4.2** **4.2**

Device Name	Model Number	Proc-essor	WiFi	Cellular	Bluetooth
	A1823 (WiFi + cellular)		**802.11/a/b/g/ n/ac**	**See Table 3**	

Table 3: Cellular Protocols Supported

Device Name	Model Number	Cellular
iPhone 5s	**A1533 (GSM)**	**UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz);** **LTE (Bands 1, 2, 3, 4, 5, 8, 13, 17, 19, 20, 25)**
	A1533 (CDMA)	**CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz);** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz);** **LTE (Bands 1, 2, 3, 4, 5, 8, 13, 17, 19, 20, 25)**
	A1453	**CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz);** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz);** **LTE (Bands 1, 2, 3, 4, 5, 8, 13, 17, 18, 19, 20, 25, 26)**

	A1457	**UMTS/HSPA+/DC-HSDPA (850, 900, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz);** **LTE (Bands 1, 2, 3, 5, 7, 8, 20)**
	A1530	**UMTS/HSPA+/DC-HSDPA (850, 900, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz);** **FDD-LTE (Bands 1, 2, 3, 5, 7, 8, 20);** **TD-LTE (Bands 38, 39, 40)**
iPhone 6 Plus/ iPhone 6	**A1549/A1522 (GSM)**	**UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)**
	A1549/A1522 (CDMA)	**CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)**

	A1586/A1524	**CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **TD-SCDMA 1900 (F), 2000 (A)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)** **TD-LTE (Bands 38, 39, 40, 41)**
iPhone 6S Plus/ **iPhone 6S**	**A1634/A1633 (US)**	**CDMA EV-DO Rev. A (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **TD-SCDMA 1900 (F), 2000 (A)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)** **TD-LTE (Bands 38, 39, 40, 41)**
	A1687/A1688 (Global)	**CDMA EV-DO Rev. A (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **TD-SCDMA 1900 (F), 2000 (A)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29)** **TD-LTE (Bands 38, 39, 40, 41)**

iPhone 7 Plus/ **iPhone 7**	**A1784/A1778 (GSM)**	**UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)** **TD-LTE (Bands 38, 39, 40, 41)**
	A1661/A1660 (CDMA)	**CDMA EV-DO Rev. A (800, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **TD-SCDMA 1900 (F), 2000 (A)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)** **TD-LTE (Bands 38, 39, 40, 41)**
iPhone SE	**A1662 (US)**	**CDMA EV-DO Rev. A (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 8, 12, 13, 17, 18, 19, 20, 25, 26, 29)**
	A1723 (Global)	**CDMA EV-DO Rev. A (800, 1700/2100, 1900, 2100 MHz)** **UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)** **TD-SCDMA 1900 (F), 2000 (A)** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 17, 18, 19, 20, 25, 26, 28)** **TD-LTE (Bands 38, 39, 40, 41)**

iPad mini 2	**A1490**	**UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26)**
	A1491	**UMTS (WCDMA)/HSPA+/ DC-HSDPA (850, 900, 1900, 2100 MHz),** **GSM/EDGE (850, 900, 1800, 1900 MHz),** **TD-SCDMA (1900 (F), 2000 (A))** **LTE (Bands 1, 2, 3, 5, 7, 8, 18, 19, 20)** **TD-LTE (Bands 38, 39)**
iPad mini 3	**A1600**	**UMTS/HSPA/HSPA+/DC‑HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26)**
	A1601	**UMTS/HSPA/HSPA+/DC‑HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **CDMA EV-DO Rev. A (800, 1900 MHz)** **TD-SCDMA (1900 (F), 2000 (A))** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 18, 19, 20)** **TD-LTE (Bands 38, 39, 40)**

iPad mini 4	**A 1550**	**UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29, 38, 39, 40, 41)**
iPad Air	**A1475**	**UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz);** **GSM/EDGE (850, 900, 1800, 1900 MHz)** **CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26)**
	A1476	**UMTS (WCDMA)/HSPA+/ DC-HSDPA (850, 900, 1900, 2100 MHz),** **GSM/EDGE (850, 900, 1800, 1900 MHz), TD-SCDMA (1900 (F), 2000 (A))** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26)** **TD-LTE (Bands 38, 39)**
iPad Air 2	**A1567**	**GSM/EDGE (850, 900, 1800, 1900 MHz),** **UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz),** **CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz),** **TD-SCDMA** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17,18, 19, 20, 25, 26, 28, 29)** **TD-LTE (Bands 38, 39, 40,41)**

iPad Pro 12.9”	**A1652**	**CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29, 38, 39, 40, 41)**
iPad Pro 9.7”	**A1674**	**CDMA EV-DO Rev. A and Rev. B (800, 1900 MHz)** **UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE Advanced (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30, 38, 39, 40, 41)**
iPad	**A1823**	**CDMA EV-DO Rev. A and Rev. B** **UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz)** **LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 38, 39, 40, 41)**

3.2 Physical Scope of the TOE

The TOE is a Mobile Device which is composed of a hardware platform and its system software. It provides wireless connectivity and includes software for VPN connection, for access to the protected enterprise network, enterprise data and applications, and for communicating to other Mobile Devices. The software for the VPN connection is evaluated separately.

The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. The TOE may be used as a mobile device within an enterprise environment where the configuration of the device is managed through an evaluated MDM solution.

The TOE communicates and interacts with IEEE 802.11-2012 Access Points and mobile data networks to establish network connectivity. Via the established network connection, the TOE is able to communicate with an MDM server allowing administrative control of the TOE.

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

4.1 Cryptographic Support

The TOE provides cryptographic services via two cryptographic modules as follows.

- The Apple iOS CoreCrypto Kernel Module v7
- The Apple iOS CoreCrypto Module v7

The iOS CoreCrypto Kernel Module is an iOS kernel extension optimized for library use within the iOS kernel. Once the module is loaded into the iOS kernel its cryptographic functions are made available to iOS Kernel services only.

The iOS CoreCrypto Module is designed for library use within the iOS user space. It is implemented as an iOS dynamically loadable library. The dynamically loadable library is loaded into the iOS application and its cryptographic functions are made available to the application.

The cryptographic functions provided include symmetric key generation, encryption and decryption using the Triple-DES and advanced encryption standard (AES) algorithms, asymmetric key generation and key establishment, cryptographic hashing, and keyed-hash message authentication.

For a list of cryptographic services provided by those modules, see the related FIPS 140-2 Security Policy documents.

Those functions are used to implement the security protocols supported as well as for the encryption of data-at-rest.

4.2 User Data Protection

User data in files is protected using cryptographic functions, ensuring this 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 provide additional protection. Password protection and encryption ensure that data-at-rest remains protected even in the case the device is lost or stolen.

Data can also be protected such that only the application that owns the data can access it.

4.3 Identification and Authentication

Except for making emergency calls users need to authenticate using a password. This password can be configured for a minimum length, for dedicated password policies and for a maximum life time. When entered, passwords are obscured and the frequency of entering passwords is limited as well as the number of consecutive failed attempts of entering the password. The TOE also enters a locked state after a (configurable) time of user inactivity and the user is required to enter his password to unlock the TOE.

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

4.4 Security Management

The security functions listed in Table 1 can be managed either by the user or by an authorized administrator through a Mobile Device Management system. Table 3 in the "Apple iOS 10.2 PP_MD_V3.0, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target" identifies the functions that can be managed and indicates, if the management can be performed by the user, by the authorized administrator, or both.

4.5 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—keys used for TOE internal key wrapping and for the protection of data-at-rest are not exportable. There are special provisions for fast and secure wiping of key material.
- Use of memory protection and processor states to separate applications and protect the TSF from unauthorized access to TSF resources—in addition each device includes a separate system called the "secure enclave" which is the only system that can use the Root Encryption Key.
- Digital signature protection of the TSF image—all updates to the TSF need to be digitally signed.
- Software/firmware integrity self-test upon start-up—the TOE will not go operational when this test fails.
- Digital signature verification for applications
- Access to defined TSF data and TSF services only when the TOE is unlocked

4.6 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.

4.7 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
- TLS
- IPsec

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for Mobile Device Fundamentals, Version 3, the Extended Package for Mobile Device Management Agents Version 3.0 and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients Version 1.0. That information has not been reproduced here and the PP_MD_V3.0, EP_MDM_AGENT_V3.0 and PP_WLAN_CLI_EP_V1.0 should be consulted if there is interest in that material.

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.

The scope of this evaluation was limited to the functionality and assurances covered in the relevant Protection Profiles and applicable NIAP technical decisions as described for this TOE in the Security Target. This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process. 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.

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 relevant Protection Profiles and performed by the evaluation team).

6. Documentation

The following documentation was used as evidence for the evaluation of the Apple iOS 10.2.

6.1 Design Documentation

None

6.2 Guidance Documentation

The following documentation was used as evidence for the evaluation.

"Apple iOS 10 Common Criteria Guide," Version 1.0

iPhone User Guide for iOS 10.2 [iPhone_UG] iBooks Link (iPhone 10.2): https://itunes.apple.com/us/book/iphone-user-guide-for-ios-10.2/id1134772174?mt=11

iPad User Guide for iOS 10.2 [iPad_UG] iBooks Link (iPad 10.2): https://itunes.apple.com/us/book/ipad-user-guide-for-ios-10.2/id1134772572?mt=11

Administrator Guidance iOS Deployment Reference [iOSDeployRef] https://itunes.apple.com/us/book/ios-deployment-reference/id917468024?mt=11

Configuration Profile Reference [IOS_CFG] https://developer.apple.com/enterprise/ConfigurationProfileReference.pdf

Apple Configurator 2 Help (online guidance) [AConfig] http://help.apple.com/configurator/mac/2.2/

Apple Deployment Programs Device Enrollment Program Guide [DEP_Guide] https://www.apple.com/ae/business/docs/DEP_Guide.pdf

Profile Manager Help [PM_Help] https://help.apple.com/profilemanager/mac/5.1/#/apdB8464D5D-F4C9-4848-9AD7-4B188ED6E130

Profiles and Logs [IOS_LOGS] https://developer.apple.com/bug-reporting/profiles-and-logs/?platforms=ios

App Developer Guidance Certificate, Key, and Trust Services Programming Guide [CKTSPG] https://developer.apple.com/library/mac/documentation/Security/Conceptual/CertKeyTrustProgGuide/01introduction/introduction.html

Certificate, Key, and Trust Services Reference [CKTSREF] https://developer.apple.com/library/content/documentation/Security/Conceptual/CertKeyTrustProgGuide/

Cryptographic Services Guide [CRYPTOGUIDE] https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html

Mobile Device Management Protocol Reference [iOS_MDM] https://developer.apple.com/library/content/documentation/Miscellaneous/Reference/MobileDeviceManagementProtocolRef/1-Introduction/Introduction.html

Information Property List Key Reference [IPLKEYREF]
https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Introduction/Introduction.html

Keychain Services Programming Guide [KEYCHAINPG]
https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/01introduction/introduction.html

Secure Framework Reference [SECFWREF]
https://developer.apple.com/library/prerelease/ios/documentation/Security/Reference/SecurityFrameworkReference/index.html

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

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the evaluation sensitive "Test Plan and Detailed Test Report, Apple iOS, Version 10.2", which is synopsized in the available Assurance Activity Report.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The devices within one device family (one device family is one row in the hardware listing of the ST) only differ in the hardware components that they provide, such as including or excluding cellular support or support for different types of cellular support (GSM versus CDMA). The security functions specified in the ST are all implemented above the layer of the hardware.

In addition, the implementation of the software managing all security functions only differs for different CPU types. This implies, with respect to the security functionality, that the devices with the same CPU type are all a different form factor of the same device. Therefore, the security functionality is not anticipated to differ between devices of the same CPU.

This list of CPUs is used as a driver to define the set of hardware used for testing of the TOE. One hardware device listed in the ST covering one of the listed CPUs is used for testing. The following list specifies the hardware used for testing:

- Apple iPad Mini 2 / iPhone5S (representative for A7)
- Apple iPad Mini 4 / iPhone 6 Plus (representative for A8)
- Apple iPad Air 2 (representative for A8X)
- Apple iPhone 6S / iPhone 6S Plus (representative for A9)

- Apple iPad Pro 9.7" (representative for A9X)
- Apple iPhone 7 / iPhone 7 Plus (representative for A10)

The test system is initially set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance supplemented by configurations required to perform testing. All individual tests are provided with detailed steps to follow by the tester.

The testing is performed by setting up a Linux server that operates as:

- Access point
- VPN endpoint
- Web server with TLS support
- Key generator
- Bluetooth endpoint

The Linux system is equipped with the appropriate tools to perform sniffing of the different traffic types and analyzing the traffic.

In addition, an Apple system is used with Apple Configurator to create the configuration profiles/policies and deploy the profiles/policies onto the different test systems. This Apple system is also equipped with the Apple Server software stack including the Apple Profile Manager. The Apple Profile Manager software component acts as the MDM server to which the test devices were connected.

The test requirements defined in the MDFPP as well as the MDMAgent EP and the WLAN EP are supplemented with detailed test instructions to ensure repeatable test activities.

The FCS_CKM_EXT.3.2 (d) requirement and assurance activity were updated by NIAP/CCEVS to allow for the extraction-then-expansion key derivation procedure as specified in SP 800-56C. The AA were re-written to align with HMAC-based Extract-and-Expand Key Derivation Function (HKDF). The lab test team was instructed to use the updated SFR and AA for this evaluation.

8. Evaluated Configuration

The guidance documentation provided specific instructions for creating configuration profiles that configured Apple iOS to comply with the functions defined in the Security Target.

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 the MDFPP , MDM Agent EP and WLAN EP received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 4 and CEM Version 3.1 Revision 4. The evaluation determined the Apple iOS 10.2 TOE to be Part 2 extended, and to meet the assurance requirements defined by the MDFPP MDM Agent EP and WLAN EP.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activities specified in the MDFPP, MDM Agent EP and WLAN EP. 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 10.2 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 MDFPP, MDM Agent EP and WLAN EP and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activities specified in the MDFPP, MDM Agent EP and WLAN EP. 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 of these 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 MDFPP, MDM Agent PP and WLAN EP and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activities specified in the MDFPP , MDM Agent EP and WLANEP. 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 is able to identify the evaluated TOE.

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 MDFPP, MDM Agent EP, and WLAN EP and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit and assurance activities specified in MDFPP, MDM Agent EP and WLAN EP. 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 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 MDFPP, MDM Agent EP, and WLAN EP and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each VAN CEM work unit and assurance activities specified in the MDFPP, MDMPP and WLAN EP. The vendor has provided security updates to the TOE during the evaluation, therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates 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 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 MDFPP, MDM Agent EP and WLAN EP and that the conclusion reached by the evaluation team was justified.

9.7 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 MDFPP, MDM Agent EP and WLAN EP and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team'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 MDFPP, MDM Agent EP and WLAN EP and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

The security functionality that was evaluated was scoped exclusively to the security functional requirements as specified in the Security Target. The VPN capabilities provided by the product were not evaluated as part of this evaluation, the VPN is being evaluated separately.
Note that there may be security functions, protocols and software offered by the devices that were not subject to evaluation and therefore are considered to be outside the evaluated configuration. No further conclusions can be drawn about their correct operation or effectiveness. The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation neither covers, nor endorses, the use of any particular MDM solution; only the MDM interfaces of the products were exercised as part of the evaluation.

11. Annexes

Not applicable.

12. Security Target

The Security Target is identified as Apple iOS 10.2 PP_MD_V3.0, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target Version 2.0, July 27, 2017

13. Glossary

The following definitions are used throughout this document.

Common Criteria Testing Laboratory (CCTL)	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.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
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.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	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.
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.

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 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
- Protection Profile for Mobile Device Fundamentals, Version 3, 10 June 2016.
- Extended Package for Mobile Device Management Agents, Version 3.0, 2016-11-21
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016