National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Apple, Inc.

Apple iOS 9.3.2 with MDM Agent

Report Number: CCEVS-VR-10725-2016
Dated: July 18, 2016 Version: 3

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

Patrick Mallett

MITRE Corporation

Kenneth B. Stutterheim

Herbert J. Ellis

Aerospace Corporation

Lucinda Hollingsworth

NIAP

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 9.3.2 with MDM Agent 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 May, 2016. 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. Those reports are summarized in the Assurance Activity Report, Version 1.2, July 14, 2016. 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 2.0, dated 17 September 2014 (PP_MD_V2.0) and the Extended Package for Mobile Device Management Agents Version 2.0 (PP_MDM_AGENT_V2.0), dated 31 December, 2014.

The TOE is the:

- Apple iOS 9.3.2 with MDM Agent on iPhone and iPad devices using the
    - A7 processor (iPhone 5s, iPad mini 2, iPad mini 3, iPad Air),
    - A8/A8X processor (iPhone 6, iPhone 6 Plus, iPad mini 4 (A8), iPad Air 2 (A8X)).
- The associated TOE guidance documentation

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)”. 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, observed evaluation 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). Therefore 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 requirements specified by the PP_MD_V2.0 and the PP_MDM_AGENT_V2.0 have been met.

The technical information included in this report was obtained from the Apple iOS 9.3 PP_MD_V2.0 & PP_MDM_AGENT_V2.0 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 CCTLs using the CEM and methodologies specified in the Protection Profiles (PP), and by the CCEVS, 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.

Table 1 provides information needed to completely identify the product, including the following items.

- The TOE: the fully qualified identifier of the product as evaluated
- The ST: describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP 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 9.3.2 on iPhone and iPad devices using the • A7 processor (iPhone 5s, iPad mini 2, iPad mini 3, iPad Air) • A8/A8X processor (iPhone 6, iPhone 6 Plus, iPad mini 4 (A8), iPad Air 2 (A8X)). The associated TOE guidance documentation is found in Section 6.2 of this document.
PP	Protection Profile for Mobile Device Fundamentals, version 2.0, 17 September 2014 and the Extended Package for Mobile Device Management Agents Version 2.0, 31 December, 2014

Item	Identifier
ST	Apple iOS 9.3.2 PP_MD_V2.0 & PP_MDM_AGENT_V2.0 Security Target Version 2.08, Date 2016-07-14
ETR	Evaluation Technical Report For Apple iOS 9.3.2 with MDM Agent
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	Sheldon Durrant, Patrick Mallett, MITRE Corporation Kenneth Stutterheim, Herb Ellis, Aerospace Corporation Lucinda Hollingsworth, NIAP

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-level layers contain fundamental services and technologies. Higher-level layers build upon the lower layers and provide more sophisticated services and technologies.

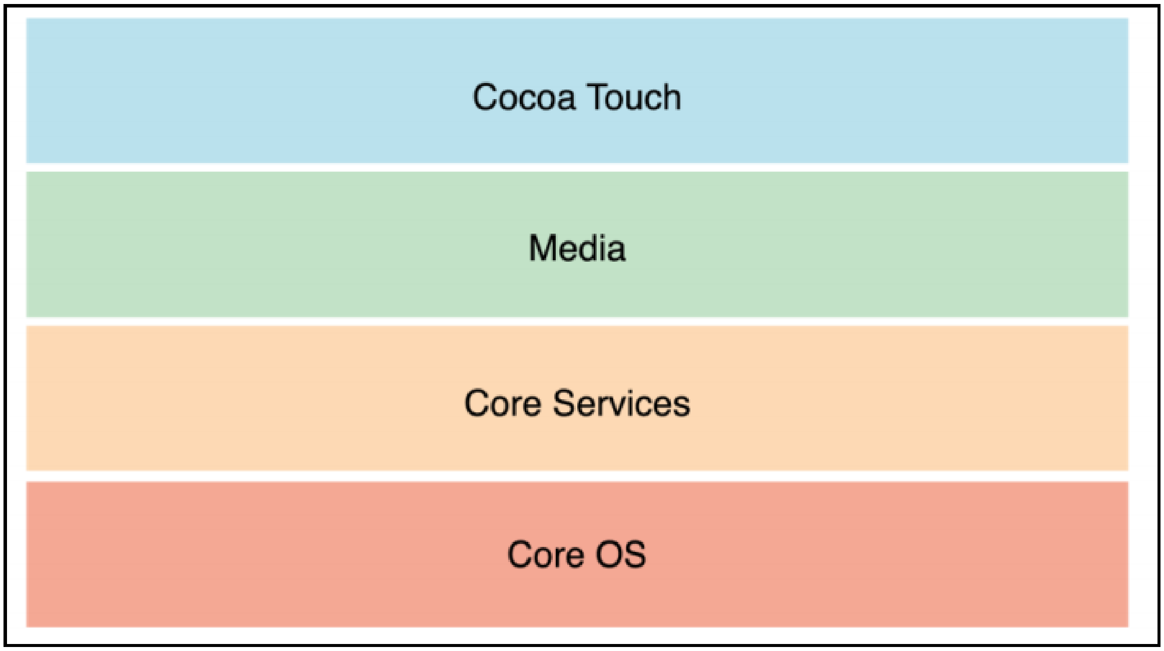

Figure 1: Layers of iOS

The individual layers provide the following services.

The **Cocoa Touch layer** contains key frameworks for building iOS applications (apps). These frameworks define the appearance of apps. The **Media layer** contains the graphics, audio, and video technologies used 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 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.

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. In situations where an app needs to explicitly deal with security or communication with an external hardware accessory, it does so by using the frameworks in the Core OS 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
- 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. It is therefore responsible for separating apps from each other and controls the use of low-level resources

The TOE may be managed by a Mobile Device Management (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 9.3.2 with MDM Agent 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)	A7	802.11/a/b/g/n/ac	See table 2	4.0
	A1533 (CDMA)		802.11/a/b/g/n/ac	See table 2	4.0
	A1453		802.11/a/b/g/n/ac	See table 2	4.0
	A1457		802.11/a/b/g/n/ac	See table 2	4.0
	A1530		802.11/a/b/g/n/ac	See table 2	4.0
iPhone 6 Plus/ iPhone 6	A1549/A1522 (GSM)	A8	802.11/a/b/g/n/ac	See table 2	4.0
	A1549/A1522 (CDMA)		802.11/a/b/g/n/ac	See table 2	4.0
	A1586/A1524		802.11/a/b/g/n/ac	See table 2	4.0
iPad mini 2	A1489 (WiFi only)	A7	802.11a/b/g/n	-	4.0
	A1490 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
	A1491 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
iPad mini 3	A1599 (WiFi only)	A7	802.11a/b/g/n	-	4.0
	A1600 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
	A1601 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
iPad mini 4	A1538 (WiFi only)	A8	802.11a/b/g/n	-	4.2
	A1550 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.2
iPad Air	A1474 (WiFi only)	A7	802.11a/b/g/n	-	4.0
	A1475 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
	A1476 (WiFi + cellular)		802.11a/b/g/n	See table 2	4.0
iPad Air 2	A1566 (WiFi only)	A8X	802.11a/b/g/n/ac	-	4.2
	A1567 (WiFi + cellular)		802.11a/b/g/n/ac	See table 2	4.2

Table 2: 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)

Device Name	Model Number	Cellular

	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)

Device Name	Model Number	Cellular
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)

Device Name	Model Number	Cellular
	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)

3.1.1 Technical Decisions

The following technical decisions were found to be applicable to the TOE:

[TD0080] Correction in TSS Assurance Activity for FMT_UNR_EXT.1.1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=83

[TD0079] RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=82

[TD0064] Whitelisting SSIDs (FMT_SMF_EXT.1, function 6) in MDF PP v2.0
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=67

[TD0060] FDP_IFC_EXT.1 & FMT_SMF_EXT.1 Function 3
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=63

[TD0059] FCS_SRV_EXT.1 & CAVS
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=62

[TD0058] MDFPP v2.0 FMT_SMF_EXT.1, function 15
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=61

[TD0057] Update to TD0047 for Non Wear Leveled Flash Memory
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=50

[TD0048] Curve25519 Implementations in FDP_DAR_EXT.2.2 Requirement
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=51

[TD0044] Update to FMT_SMF_EXT.1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=47

[TD0038] Asymmetric KEKs (including the REK) in MDFPP v1.1 and v2.0
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=41

[TD0034] Revision of Test 5 in FCS_TLSC_EXT.1.1 & EXT.2.1 reqs in MDF PP V2.0, MDM PP V2.0, MDM Agent PP V2.0
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=36

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. The TOE is used as a mobile device within an enterprise environment where the configuration of the device is managed through a compliant device management solution.

3.3 Unevaluated Security Functionalities

The following security functionalities were not evaluated as part of the iOS 9.3.2 TOE and are considered outside of the scope of the evaluation.

3.3.1 Two-Factor Authentication

According to the [iPad_UG] and the [iPhone_UG], two-factor authentication is an extra layer of security for Apple ID designed to ensure that all photos, documents, and other important data the user stored with Apple can be accessed only by the user and only with the user's device. It's built into iOS 9 and OS X EL Capitan. This feature is outside the scope of the evaluated configuration.

3.3.2 Touch ID

According to the [iPad_UG] and the [iPhone_UG], Touch ID allows the user to unlock the device by placing a finger on the Home button. This feature is provided on iPad Air 2, iPad Pro, iPad mini 3 and later, and on iPhone 5s and later. This feature is outside the scope of the evaluated configuration.

3.3.3 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.

3.3.4 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], is 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

3.3.5 VPN Split Tunnel

VPN split tunnel is outside of the evaluated configuration.

4. Security Policy

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

1. Hardware Protection Functions
2. Security audit
3. Cryptographic support
4. User data protection
5. Identification and authentication
6. Security management
7. Protection of the TSF (TOE Security Functionality)
8. TOE access
9. Trusted path/channels

4.1 Hardware Protection Functions

The Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple A7, A8 and A8X processors. It utilizes its own secure boot and personalized software update separate from the application processor. It provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised

Memory Protection

iOS uses the read and write protection for memory pages provided by the advanced Reduced Instruction Set (RISC) machine (ARM) processor for separating applications from the kernel and to provide a sandbox for each application.

4.2 Security Audit

MDM Agent Alerts

The MDM agent generates and sends an alert in response to an MDM server request (i.e., applying a policy, receiving a reachability event)

4.3 Cryptographic Support

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

- The Apple iOS CoreCrypto Kernel Module v6
- The Apple iOS CoreCrypto Module v6

Refer to the ST for specific certificate information.

4.4 User Data Protection

When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible. However all files in all classes are encrypted. 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 provides 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.

4.5 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.

4.6 Security Management

Since all the Mobile Devices specified use iOS, there are no differences between supported management functions and policies between the different mobile devices. The supported management functions are described in Table 3, *Management Functions*, of the Apple iOS 9.3 PP_MD_V2.0 & PP_MDM_AGENT_V2.0 ST.

4.7 Protection of the TOE Security Functionality (TSF)

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

- Secure Boot helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices.

- Secure Software Updates are delivered wirelessly to users who receive update notifications that encourage rapid adoption of the latest security fixes.
- Domain isolation ensures that all applications are executed in their own domain and are restricted from accessing files stored by other applications and from making device configuration changes.
- Device Locking occurs after a configurable time of inactivity or upon request of the user. The TOE can be locked remotely either via the iCloud "Lost Mode" function or by an MDM system if the device is enrolled in management.
- Time which can be GPS time or NTP time is used by several security functional requirements.
- Inventory of TSF Binaries and Libraries provides that all user space binaries are subject to address space layout randomization.
- 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 (REK). The Secure Enclave is a separate CPU that executes a stand-alone operating system and has separate memory.
- 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

4.8 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.

4.9 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 2 and in the Extended Package for Mobile Device Management Agents Version 2.0. That information has not been reproduced here and the MDFPP should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the MDFPP and extended package for MDM Agents as described for this TOE in the ST. 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 the assurance specified in PP_MD_V2.0, PP_MDM_AGENT_V2.0, and performed by the evaluation team. This evaluation only covers those specific device models and software version identified in this document and not any earlier or later versions released or in process. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6. Documentation

The following documentation was used as evidence for the evaluation of the Apple iOS 9.3.2 with MDM Agent

6.1 Design Documentation

None

6.2 Guidance Documentation

The following documentation was used as evidence for the evaluation of the Apple iPhone. All URLs were verified 2016-07-18.

- Apple Configurator 2 Help (on-line guidance: http://help.apple.com/configurator)

- Apple iOS 9.3.2 PP_MD_V2.0 & PP_MDM_AGENT_V2.0 Common Criteria Guide v2.2 (2016-07-11)
- Certificate, Key, and Trust Services Programming Guide (2014-07-15)
- Certificate, Key, and Trust Services Reference (on-line guidance: https://developer.apple.com/library/ios/documentation/Security/Reference/certifkeytrustservices/index.html)
- Cryptographic Services Guide (2013-01-28)
- Apple Deployment Programs Device Enrollment Program Guide (October 2015)
- Technical Note TN 2232: HTTPS Server Trust Evaluation (on-line guidance: https://developer.apple.com/library/ios/technotes/tn2232/_index.html)
- iPhone User Guide for iOS 9.3 (Sept 16, 2015)
- iPad User Guide for iOS 9.3 (Sept 16, 2015)
- Information Property List Key Reference (on-line guidance: https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Introduction/Introduction.html)
- Configuration Profile Reference (October, 2015)
- iOS Deployment Reference (2016)
- Mobile Device Management Protocol Reference (on-line guidance, requires Apple Developer ID: https://developer.apple.com/go/?id=mobile-device-management-protocol-reference)
- iOS Manual Pages (on-line guidance: https://developer.apple.com/library/ios/documentation/System/Conceptual/ManPages_iPhoneOS/)
- Keychain Services Programming Guide (2014-02-11)
- Profile Manager Help (on-line guidance: http://help.apple.com/profilemanager/)
- Security Framework Reference (on-line guidance: https://developer.apple.com/library/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 “Test Plan and Detailed Test Report Apple iOS 9.3.2 with MDM Agent, 2016-06-30.” That information is summarized in the Assurance Activity Report, Version 1.2, 2016-07-14

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 tests were performed on three mobile devices which were selected by choosing one from within each device family.

One device family is defined by the hardware that impacts the TSF operation: the CPU. The other hardware, such as form factor, size of non-volatile storage, presence or absence of modem devices like GSM, CDMA or LTE do not affect the TSF. All TSF functions are solely implemented in software which 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 on all devices and therefore on all CPUs equally. In addition, the security functions specified in the ST are all implemented above the hardware layer. That is, once a request is processed by the hardware, the security relevant decisions have been already made by the software. The hardware now only needs to enforce the functionality requested by the software.

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:

- iPhone5S (representative for A7)
- iPhone6 Plus (representative for A8)
- iPad Air 2 (representative for A8X)

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.

8. Evaluated Configuration

The TOE is part of a Commercial Off the Shelf System (COTS) and distributed either as already installed software on a device via retail channels, or which can be downloaded from Apple using a proprietary protocol.

The TOE is installed and configured precisely as specified in the Common Criteria Guide. The guidance documentation provides specific instructions for creating configuration profiles that configure Apple iOS to comply with the functions defined in the ST.

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 DTR.

All work units defined by the PP_MD_V2.0 and PP_MDM_AGENT_V2.0 and the CEM 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.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activities specified in the PP_MD_V2.0. 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 9.3.2 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 PP_MD_V2.0 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 document as well as functional descriptions referenced by the ST.

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 PP_MD_V2.0, 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 CEM and PP_MD_V2.0. 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 PP_MD_V2.0 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. 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 PP_MD_V2.0 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 and MDM Agent PP. 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 and 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 PP_MD_V2.0 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. The evaluation team ensured that the TOE does not contain 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 PP_MD_V2.0 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 PP_MD_V2.0 and PP_MDM_AGENT_V2.0 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, PP_MD_V2.0 and PP_MDM_AGENT_V2.0, and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

None

11. Annexes

Not applicable.

12. Security Target

The Security Target is identified as Apple iOS 9.3.2 PP_MD_V2.0 & PP_MDM_AGENT_V2.0 Security Target version 2.08.

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.
- [PP_MD_V2.0] U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals, Version 2.0 https://www.niap-ccevs.org/pp/PP_MD_v2.0/
- [PP_MDM_AGENT_V2.0] U.S. Government Approved Protection Profile - Extended Package for Mobile Device Management Agents Version 2.0 https://www.niap-ccevs.org/pp/PP_MDM_AGENT_V2.0/