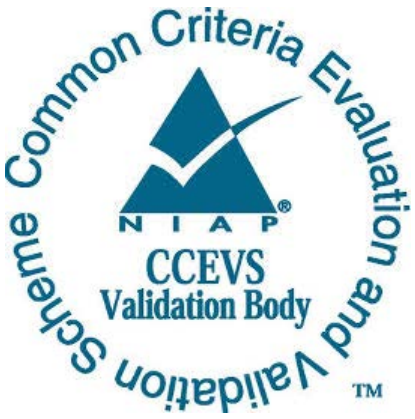
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
Apple, Inc.

Apple iOS 9.2

Report Number: CCEVS-VR-VID10695-2016
Dated: January 28, 2016 Version: 1.1

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

Members from:

The Aerospace Corporation

The MITRE 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 the iOS 9.2 mobile device 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 December, 2015. 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 set forth in the Mobile Device Fundamentals Protection Profile version 2.0.

The TOE is the Apple iOS 9.2 operating system executing on a wide selection of mobile device hardware components, as follows.

- iPhone 6 Plus / iPhone 6
- iPhone 5s
- iPad mini 3
- iPad Air 2
- iPad mini 2
- iPad Air

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, 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 CC requirements specified by the "Mobile Device Fundamental Protection Profile" (MDFPP) version 2.0 have been met.

The technical information included in this report was obtained from the Apple iOS 9.2 MDFPPv2 Security Target (ST) and analysis performed by the evaluation team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 Level (EAL) 1 through 4 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 Profile 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 9.2 executing on the following hardware: • iPhone 6 Plus / iPhone 6 • IPhone 5s • iPad mini 3 • iPad Air 2 • iPad mini 2 • iPad Air
PP	Protection Profile for Mobile Device Fundamentals, version 2.0, 17 September

Item	Identifier
	2014
ST	Apple iOS 9.2 MDFPP v2 Security Target, Version 1.4, Date 2016-1-28
ETR	Evaluation Technical Report For Apple iOS 9.2 on iPhone and iPad
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 Validation Team	Comprised of members from The Aerospace Corporation and MITRE 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.

The individual layers provide the following services.

The Cocoa Touch layer contains key frameworks for building iOS applications (apps). The Media layer contains the graphics, audio, and video technologies to implement multimedia in apps.

The Core Services layer contains fundamental system services for apps. 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 take advantage of the built-in encryption available. 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 is intended to be part of a mobile device management (MDM) solution that enables the enterprise to control and administer all TOE instances that are part of the enterprise MDM solution.

3.1 TOE Evaluated Configuration

The evaluation covers Apple iOS 9.2 on the following mobile devices as detailed in Tables 2 and 3, below.

Table 2: Devices Covered by the Evaluation

Device Name	Model Number	WiFi	Cellular	Bluetooth
iPhone 6 Plus/ iPhone 6	A1549/A1522 (GSM)	802.11/a/b/g/n/ac	See table	4.0
	A1549/A1522 (CDMA)	802.11/a/b/g/n/ac	See table	4.0
	A1586/A1524	802.11/a/b/g/n/ac	See table	4.0
iPhone 5s	A1533 (GSM)	802.11/a/b/g/n/ac	See table	4.0
	A1533 (CDMA)	802.11/a/b/g/n/ac	See table	4.0
	A1453	802.11/a/b/g/n/ac	See table	4.0
	A1457	802.11/a/b/g/n/ac	See table	4.0
	A1530	802.11/a/b/g/n/ac	See table	4.0
iPad mini 3	WiFi only	802.11a/b/g/n	-	4.0
	WiFi + cellular	802.11a/b/g/n	See table	4.0
iPad Air 2	WiFi only	802.11a/b/g/n/ac	-	4.0
	WiFi + Cellular	802.11a/b/g/n/ac	See table	4.0
iPad mini 2	WiFi only	802.11a/b/g/n	-	4.0
	WiFi + Cellular	802.11a/b/g/n	See table	4.0

Device Name	Model Number	WiFi	Cellular	Bluetooth
iPad Air	WiFi only	802.11a/b/g/n	-	4.0
	WiFi + Cellular	802.11a/b/g/n	See table	4.0

Table 3: Cellular Protocols Supported

Device Name	Model Number	Cellular
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
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)
iPad mini 3	WiFi + cellular	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)
iPad Air 2	WiFi + cellular	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 mini 2	WiFi + cellular	UMTS/HSPA/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz)

Device Name	Model Number	Cellular
		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)
iPad Air	WiFi + cellular	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)

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 communication with other Mobile Devices.

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

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and the through that connectivity interacts with MDM servers that allow 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. Secure management
6. Protection of the TSF (TOE Security Functionality)
7. TOE access

4.1 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

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.

Note: Both modules are currently in the process of being FIPS 140-2 validated in a configuration that is compliant with the TOE defined in the Security Target. Older versions of both modules have been FIPS 140-2 validated.

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.

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 to ensure 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.

4.3 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 password entry is configurable. 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 9.2 MDFPPv2 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 enter an operational state 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, which is addressed in a separate evaluation

5. Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for Mobile Device Fundamentals, Version 2. 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 Version 2.0, dated 17 September 2014 and associated technical decisions 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 Mobile Device Fundamentals Protection Profile 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 9.2.

6.1 Design Documentation

None

6.2 Guidance Documentation

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

- "iOS Security iOS 9.0" or later, September 2015
- "iOS Technology Overview"
- "iPhone User Guide for iOS 9.2"
- "iPad User Guide for iOS 9.2"
- "Configuration Profile Reference," October 8, 2015
- "iOS Deployment Reference"
- "Apple iOS 9.2 Common Criteria Guide," Version 1.6

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 proprietary "Evaluation Team Test Report for the Apple iOS 9.2," Version 1.2, 2016-1-28.

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.

With the aforementioned considerations, testing is performed on the following devices. The devices listed in parentheses are implicitly covered by the testing on the given device considering the aforementioned discussion: iPhone5S (all iPhone5S listed in the ST, iPad Air, iPad mini 2, iPad mini 3), iPhone6 Plus (all iPhone6 and iPhone6 Plus devices listed in ST) and iPad Air 2.

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.

The test requirements defined in the MDFPP are supplemented with detailed test instructions to ensure a repeatable testing.

8. Evaluated Configuration

The guidance documentation provides specific instructions for creating configuration profiles that configure the Apple iOS 9.2 mobile devices to comply with the functions defined in the Security Target. The TOE must be configured as described in Apple iOS 9 Common Criteria Guide document to be in the evaluated configuration.

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 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 9.2 TOE to be Part 2 extended, and to meet the assurance requirements defined by the MDFPP.

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. 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 9.2 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 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 MDPFF. 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 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 MDFPP 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. 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 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 MDFPP 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 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 and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

Please note the following:

- The VPN capabilities as provided by the product were not evaluated as part of this evaluation, instead those are being evaluated separately.
- There are security functions and protocols offered by the product that were not subject to evaluation and are outside the evaluated configuration as noted in the **Apple iOS 9.2 MDFPPv2 Common Criteria Guide**, **Version 1.6**, section 2.3 and no further conclusions can be drawn about their effectiveness.

11. Annexes

Not applicable.

12. Security Target

The Security Target is identified as Apple iOS 9.2 MDFPPv2 Security Target, Version 1.4, 2016-1-28.

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 2, 17 September 2014.