National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Apple iPad and iPhone Mobile Devices with iOS 11.2

Report Number: CCEVS-VR-10851-2018
Dated: March 30, 2018
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

Patrick Mallett, Ph.D.

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 Apple iOS 11 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 March, 2018. 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 3.1; 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 as amended by the relevant NIAP technical decisions for those protection profiles.

The TOE is Apple iPad and iPhone Mobile Devices with iOS 11.2 executing on the following platforms:

- iPhone 5s (A7 processor)
- iPhone 6 Plus / iPhone 6 (A8 processor)
- iPhone 6s Plus / iPhone 6s (A9 processor)
- iPhone 7 / iPhone 7 Plus (A10 Fusion processor)
- iPhone 8 / iPhone 8 Plus (A11 Bionic processor)
- iPhone X (A11 Bionic processor)
- iPhone SE (A9 processor)
- iPad mini 3 (A7 processor)
- iPad mini 4 (A8 processor)
- iPad (A9 processor)
- iPad Air 2 (A8X processor)
- iPad Pro 12.9” (A9X processor)
- iPad Pro 12.9” (A10X Fusion processor)
- iPad Pro 10.5” (A10X Fusion)
- iPad Pro 9.7” (A9X)

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the “Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)” (CEM) for

conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

The CCTL atsec information security corporation evaluation team concluded that the CC requirements specified by the Mobile Device Fundamental Protection Profile Version 3.1 (PP_MD_V3.1), the Extended Package for Mobile Device Management Agents Version 3.0 (EP_MDM_AGENT_V3.0), and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients Version 1.0 (PP_WLAN_CLI_EP_V1.0) have been met.

The technical information included in this report was obtained from the Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target (ST) Version 1.01 and analysis performed by the validation team.

2. Identification

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

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

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST): describing the security features, claims, and assurances of the product
- The conformance results of the evaluation

- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iPad and iPhone Mobile Devices with iOS 11.2 executing on the following platforms: • iPhone 5s (A7 processor) • iPhone 6 Plus / iPhone 6 (A8 processor) • iPhone 6s Plus / iPhone 6s (A9 processor) • iPhone 7 / iPhone 7 Plus (A10 Fusion processor) • iPhone 8 / iPhone 8 Plus (A11 Bionic processor) • iPhone X (A11 Bionic processor) • iPhone SE (A9 processor) • iPad mini 3 (A7 processor) • iPad mini 4 (A8 processor) • iPad (A9 processor) • iPad Air 2 (A8X processor) • iPad Pro 12.9" (A9X processor) • iPad Pro 12.9" (A10X Fusion processor) • iPad Pro 10.5" (A10X Fusion processor) • iPad Pro 9.7" (A9X processor)
PP	Protection Profile for Mobile Device Fundamentals Version 3.1, 16 June 2017 Extended Package for Mobile Device Management Agents Version 3.0, 21 November 2016 The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, dated 8 February, 2016
ST	Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target, Version 1.01, Date: 2018-03-30
ETR	Evaluation Technical Report for a Target of Evaluation Apple iPad and iPhone devices with iOS 11.2
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Apple Inc.

Item	Identifier
Developer	Apple Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Patrick Mallet, PhD., 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.

TOE Evaluated Configuration

The evaluation covers following Apple iPad and iPhone mobile devices running iOS 11 operating system as detailed in Table 1 and Table 2, below.

Table 1: Devices Covered by the Evaluation

Device Name	Model Number	Process-or	Wi-Fi	Cellular	Blue-tooth	BAF
iPhone 5s	A1533 (GSM)	A7	802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1533 (CDMA)		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1453		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1457		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1530		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
iPhone 6 Plus/ iPhone 6	A1549/A1522 (GSM)	A8	802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1549/A1522 (CDMA)		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
	A1586/A1524		802.11/a/b/g/n/ac	See table 2	4.0	Touch ID 1
iPhone 6s Plus	A1634/A1633 (US)	A9	802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 2
iPhone 6s	A1687/A1688 (Global)		802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 2
iPhone 7 Plus/	A1784/A1778 (GSM)	A10 Fusion	802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 3
iPhone 7	A1661/A1660 (CDMA)		802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 3
iPhone 8 Plus	A1864/A1898/A1899/A1897	A11 Bionic	802.11/a/b/g/n/ac	See table 2	5.0	Touch ID 3
iPhone 8	A1863/A1906/A1907/A1905		802.11/a/b/g/n/ac	See table 2	5.0	Touch ID 3
iPhone X	A1865/A1902/A1901	A11 Bionic	802.11/a/b/g/n/ac	See table 2	5.0	Face ID
			802.11/a/b/g/n/ac	See table 2	5.0	Face ID
iPhone SE	A1662 (US)	A9	802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 1
	A1723 (Global)		802.11/a/b/g/n/ac	See table 2	4.2	Touch ID 1

iPad mini 3	A1599 (Wi-Fi only) A1600 (Wi-Fi + cellular) A1601 (Wi-Fi + cellular)	A7	802.11a/b/g/n 802.11a/b/g/n 802.11a/b/g/n	- See table 2 See table 2	4.0 4.0 4.0	Touch ID 1 Touch ID 1 Touch ID 1
iPad mini 4	A1538 (Wi-Fi only) A1550 (Wi-Fi + cellular)	A8	802.11a/b/g/n 802.11a/b/g/n	- See table 2	4.2 4.2	Touch ID 1 Touch ID 1
iPad Air 2	A1566 (Wi-Fi only) A1567 (Wi-Fi + cellular)	A8X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 1 Touch ID 1
iPad Pro 12.9”	A1584 (Wi-Fi only) A1652 (Wi-Fi + cellular)	A9X	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 1 Touch ID 1
iPad Pro 9.7”	A1673 (Wi-Fi only) A1674 (Wi-Fi + cellular)	A9X	802.11/a/b/g/n/ac 802.11 /a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 1 Touch ID 1
iPad	A1822 (Wi-Fi only) A1823 (Wi-Fi + cellular)	A9	802.11/a/b/g/n/ac 802.11/a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 1 Touch ID 1
iPad Pro 12.9”	A1670 (Wi-Fi) A1671 (Wi-Fi + Cellular)	A10X Fusion	802.11/a/b/g/n/ac 802.11 /a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 3 Touch ID 3
iPad Pro 10.5”	A1701 (Wi-Fi) A1709 (Wi-Fi + Cellular)	A10X Fusion	802.11/a/b/g/n/ac 802.11 /a/b/g/n/ac	- See table 2	4.2 4.2	Touch ID 3 Touch ID 3

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)
	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)

Device Name	Model Number	Cellular
	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)

Device Name	Model Number	Cellular
	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 8 Plus/ iPhone 8	A1863/A1864	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66) TD-LTE (Bands 34, 38, 39, 40, 41) TD-SCDMA 1900 (F), 2000 (A) CDMA EV-DO Rev. A (800, 1900, 2100 MHz) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A1897	Models A1905 and A1897 do not support CDMA networks, such as those used by Verizon and Sprint. FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66) TD-LTE (Bands 34, 38, 39, 40, 41) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A1905	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66) TD-LTE (Bands 34, 38, 39, 40, 41) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone X	A1865/A1902	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66) TD-LTE (Bands 34, 38, 39, 40, 41) TD-SCDMA 1900 (F), 2000 (A) CDMA EV-DO Rev. A (800, 1900, 2100 MHz) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A1901	FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 29, 30, 66) TD-LTE (Bands 34, 38, 39, 40, 41) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)

Device Name	Model Number	Cellular
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 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 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)

Device Name	Model Number	Cellular
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)
iPad Pro 12.9”	A1671	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 Pro 10.5”	A1709	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)

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 can 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

Security Audit

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

Cryptographic Support

The TOE provides cryptographic services via the following cryptographic modules:

- The Apple iOS CoreCrypto Kernel Module v8 for ARM
- The Apple iOS CoreCrypto Module v8 for ARM

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 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 and trusted update.

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.

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

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

Identification and Authentication

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

The password can be configured for a minimum length to meet 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 either enter his password or use biometric authentication (fingerprint or face) to unlock the TOE.

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

Security Management

The security functions listed above can be managed either by the user or by an authorized administrator through a Mobile Device Management system. Table 5 of the 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.

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 Processor" (SEP) which is the only system that can use the Root Encryption Key. The SEP 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 enter into an operational mode when this test fails.
- Digital signature verification for applications.
- Access to defined TSF data and TSF services only when the TOE is unlocked.

TOE Access

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

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

Trusted Path/Channels

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

- IEEE 802.11-2012
- IEEE 802.1X
- EAP-TLS
- TLS
- IPsec (addressed in a separate evaluation)

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0. That information has not been reproduced here and the PP_MD_V3.1, EP_MDM_AGENT_V3.0 and PP_WLAN_CLI_EP_V1.0 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 PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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

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

6. Documentation

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

Design Documentation

None

Guidance Documentation

The following documentation was used as evidence for the evaluation.

User Guidance

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

Administrator Guidance

[CC_GUIDE] Apple iPad and iPhone Mobile Devices PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Common Criteria Guide	https://www.niap-ccevs.org/st/st_vid10851-agd.pdf

Supporting Documents

[iOSDeployRef] iOS Deployment Reference (V3.9)	https://itunes.apple.com/us/book/ios-deployment-reference/id917468024?mt=11
[OTA_Guide] Over-The-Air Profile Delivery and Configuration Guide (Updated 2018-01-24)	https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html
[IOS_CFG] Configuration Profile Reference (Updated 2018-01-24)	https://developer.apple.com/enterprise/ConfigurationProfileReference.pdf
[AConfig] Apple Configurator 2 Help (online guidance)	http://help.apple.com/configurator/mac/2.6//
[DEP_Guide] Apple Deployment Programs Device Enrollment Program Guide	https://www.apple.com/education/docs/DEP_Guide.pdf
[PM_Help] Profile Manager Help	https://help.apple.com/profilemanager/mac/5.4/
[IOS_LOGS] Profiles and Logs	https://developer.apple.com/bug-reporting/profiles-and-logs/?platforms=ios

App Developer Guidance

[3CC-MAN] Common Crypto man pages	https://developer.apple.com/legacy/library/documentation/Darwin/Reference/ManPages/#
[CKTSREF] Certificate, Key, and Trust Services	https://developer.apple.com/documentation/security/certificate_key_and_trust_services

[CRYPTOGUIDE] Cryptographic Services Guide	https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html
[iOS_MDM] Mobile Device Management Protocol Reference	https://developer.apple.com/library/content/documentation/Miscellaneous/Reference/MobileDeviceManagementProtocolRef/1-Introduction/Introduction.html
[IPLKEYREF] Information Property List Key Reference	https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Introduction/Introduction.html
[KEYCHAINPG] Keychain Services Programming Guide	https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/01introduction/introduction.html
[SECFWREF] Secure Framework	https://developer.apple.com/library/prerelease/ios/documentation/Security/Reference/SecurityFrameworkReference/index.html
[HTTPSTN2232] Technical Note TN 2232: HTTPS Server Trust Evaluation	https://developer.apple.com/library/ios/technotes/tn2232/_index.html

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.

Developer Testing

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

Evaluation Team Independent Testing

The ST lists many more devices compared to the set of devices used for testing. The tests were performed on a large subset of this set 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 such as 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. I.e. 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. All the devices listed in the ST use one of the following CPUs.

- A7

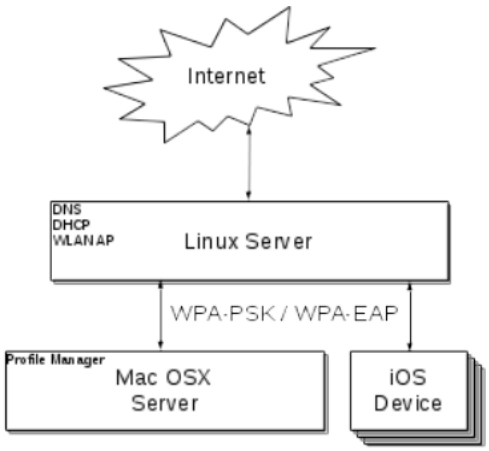
- A8
- A8X
- A9
- A9X
- A10 Fusion
- A10X Fusion
- A11 Bionic

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 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 Fusion)
- Apple iPad Pro 12.9” (representative for A10X Fusion)
- Apple iPhone 8 / iPhone 8 Plus / iPhone X (representative for A11 Bionic)

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

Test Tools and Configuration



Test Configuration

Apple Tools

- OS X 10.13 macOS Sierra
- Apple Configurator 2.5
- OS X Server 5.4 with the Apple Profile Manager

Linux Tools:

- Fedora 26 system
- Iptables Linux kernel version 1.6.0
- netcat version 7.4
- dnsmasq version 2.76
- hostapd, version 2.4
- tcpdump, version 4.9.0
- hcidump and bdaddr from the Bluez Linux Bluetooth protocol stack version 5.43.
- OpenSSL with s_server and s_client applications version 1.0.2k
- Wireshark 2.2.8 with libpcap 1.8.1
-

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

- WLAN access point,
- VPN endpoint,
- Web server with TLS support,
- Key generator, and
- Bluetooth endpoint.

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

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 PP_MD_V3.1 and EP_MDM_AGENT_V3.0 and supported by the PP_WLAN_CLI_EP_V1.0 are supplemented with detailed test instructions to ensure a repeatable testing.

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 NIST standard, IETF RFC 5869 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 provides specific instructions for creating configuration profiles that configure Apple iOS to comply with the functions defined in the Security Target. Only the documentation listed in section 6 above should be used to establish 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 and summarized in the Assurance Activity report for this evaluation.

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

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

Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0. 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 11 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

Evaluation of the Development Documentation (ADV)

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

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

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0. 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 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 the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

The evaluation team applied each ATE CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0. 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 the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 and that the conclusion reached by the evaluation team was justified.

Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1. The vendor provided

security updates to the TOE during the evaluation, therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates 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 the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 and that the conclusion reached by the evaluation team was justified.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the testing defined by the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 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 the PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0 and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

Note that the evaluation is iOS 11.2. Apple updates the iOS as necessary to address bug fixes and security issues. Once an updated iOS is released, prior versions are no longer available. In the case of this evaluation, iOS 11.2 underwent updates during the evaluation process, and the most recent version is now 11.2.6. The evaluation team worked closely with Apple regarding any effect the changes may have had upon the security functionality provided by the devices. TOE administrators are encouraged to deploy the latest patched version of the evaluated Operating System.

11. Annexes

Not applicable.

12. Security Target

The Security Target is identified as Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_V3.1, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP_V1.0 Security Target, Version 1.01 2018-03-30.

13. Glossary

The following definitions are used throughout this document.

AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CDMA	Code Division Multiple Access
CDMA EV-DO	Code Division Multiple Access Evolution-Data Optimized
CCTL	Common Criteria Testing Laboratory—An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
DC-HSDPA	Dual-Carrier High Speed Packet Access
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EP	Extended Package (for a Protection Profile)
ETR	Evaluation Technical Report
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
FDD-LTE	Frequency-Division Duplex-Long Term Evolution
Feature	Part of a product that is either included with the product or can be ordered separately.
GSM	Global System for Mobile Communication
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-hash Message Authentication Code
HSPA+	High Speed Packet Access Plus
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation—A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
TD-LTE	Time Division Long-Term Evolution

TD-SCDMA	Time Division Synchronous Code Division Multiple Access
TLS	Transport Layer Security
TSF	TOE Security Functionality
UMTS	Universal Mobile Telecommunications System
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

14. Bibliography

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

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017.
- Extended Package for Mobile Device Management Agents, Version 3.0, 21 November 2016.
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Client, Version 1.0, 08 February 2016