National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Extended Package for Mobile Device Management Agents, Version 3.0, November 21, 2016

Report Number:	**CCEVS-VR-PP-0035**
Dated:	**17 August 2017**
Version:	**1.0**

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

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

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759

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 Security Requirements for Mobile Device Management Agents (version 3.0) Extended Package, also referred to as the Mobile Device Protection Profile (EPMDMA30). It presents a summary of the EPMDMA30 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the EPMDMA30 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Apple iOS 10.2 . The evaluation was performed by the atsec information security lab Common Criteria Testing Laboratory (CCTL) in Austin, Texas, United States of America, and was completed in May 2017. This evaluation addressed the base requirements of the EPMDMA30.

Additional review of the EP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the EPMDMA v.3.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The EP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains material drawn directly from the EPMDMA30, performance of the majority of the ASE work units serves to satisfy the APE work units as well.

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 found that the evaluation showed that the EPMDMA30 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the EP.

In order to promote thoroughness and efficiency, the evaluation of the EPMDMA30 was performed concurrent with the first product evaluation against the EP. In this case the TOE for this first product was Apple iOS 10.2, provided by Apple Inc. The evaluation was performed by the atsec information security Corp. Common Criteria Testing Laboratory (CCTL) in Austin, Texas, United States of America, and was completed in May 2017.

The EPMDMA30 contains a set of "base" requirements that all conformant STs must include, and in addition, contains "Objective" requirements. Objective requirements are those that that specify security functionality that is desirable but is not explicitly required by the EP. The vendor may choose to include such requirements in the ST and still claim conformance to this EP.

Because these discretionary requirements may not be included in a particular ST, the initial use of the EP will address (in terms of the EP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the EPMDMA30 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the EP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this EP, as well as subsequent evaluations that address additional optional requirements in the EPMDMA30.

Protection Profile	*Extended Package for Mobile Device Management Agents, Version 3.0, 21 November 2016*
ST (Base)	Apple iOS 10.2 PP_MD_V3.0, EP_MDM_AGENT_V3.0, & PP_WLAN_CLI_EP Security Target, Version 2.0, July 27, 2017
Assurance Activity Report (Base)	VID10782_SER_AAR_Apple_iOS_10_v4.0, Version 4.0, July 28, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	atsec information security Corp. Austin, TX. USA
CCEVS Validators	Patrick Mallett, MITRE
	Kenneth Stutterheim, The Aerospace Corporation

3 EPMDMA Description

The EPMDMA30 describes security requirements for a Mobile Device Management (MDM) Agent and is intended to provide a minimal baseline set of requirements that are targeted at mitigating well defined and described threats. The Agent of an MDM system is only one component of an enterprise deployment of mobile devices. Other components, such as the mobile device platforms, which enforce the security policies, and servers, which host mobile application repositories, are out of scope. Compliant TOEs will provide essential services, such as audit data generation on TOE and platform, cryptographic services, and user management, and unenrollment prevention to support the secure deployment of an MDM system. The TOE will also have the ability to implement trusted policy updates.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.CONNECTIVITY	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
A.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon mobile platform and hardware evaluated against the MDFPP and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
A.PROPER_ADMIN	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
A.PROPER_USER	Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.MALICIOUS_APPS	Malicious or flawed application threats exist because apps loaded onto a mobile device may include malicious or exploitable code. An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE, resulting in the compromise of TOE or TOE data.
T.BACKUP	An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user’s backup repository, it’s not likely enterprise would detect compromise.
T.NETWORK_ATTACK	An attacker may masquerade as MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
T.NETWORK_EAVESDROP	Unauthorized entities may intercept communications between the MDM and mobile devices to monitor, gain access to, disclose, or alter remote management commands. Unauthorized entities may intercept unprotected wireless communications between the mobile device and the Enterprise to monitor, gain access to, disclose, or alter TOE data.
T.PHYSICAL_ACCESS	The mobile device may be lost or stolen, and an unauthorized individual may attempt to access user data. Although these attacks are primarily directed against the mobile device platform, the MDM Agent configures features, which address this threat.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to Mobile Devices.

Table 3: Organizational Security Policies

TOE Security Obj.	TOE Security Objective Definition
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.
P.ADMIN	The configuration of the mobile device security functions must adhere to the Enterprise security policy.
P.DEVICE_ENROLL	A mobile device must be enrolled for a specific user by the administrator of the MDM prior to being used in the Enterprise network by the user.
P.NOTIFY	The mobile user must immediately notify the administrator if a mobile device is lost or stolen so that the administrator may apply remediation actions via the MDM system.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ACCOUNTABILITY	The TOE must provide logging facilities, which record management actions undertaken by its administrators
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS and the MDM Server. This will include the initial enrollment of the device into management, through its entire lifecycle, including policy updates and its possible unenrollment from management services.
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed, or altered.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.DATA_PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner
OE.DATA_PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.
OE.IT_ENTERPRISE	The Enterprise IT infrastructure provides security for a network that is available to the TOE and mobile devices that prevents unauthorized access.
OE.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon the trustworthy mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides

Environmental Security Obj.	TOE Security Objective Definition
	trusted updates and software integrity verification of the MDM Agent.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.

5 Requirements

As indicated above, requirements in the EPMDMA30 are comprised of the "base" requirements and optional additional requirements. The following are table contains the "base" requirements that were validated as part of the Apple iOS 10.2 evaluation activity referenced above. The following table lists the TOE Security Functional Requirements/

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ALT_EXT.2: Agent Alerts	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FAU_GEN.1(2): Audit Data Generation	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FAU_SEL.1(2): Security Audit Event Selection	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FIA: Identification and Authentication	FIA_ENR_EXT.2: Enrollment of Mobile Device Management	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FMT: Security Management	FMT_POL_EXT.2: Trusted Policy Update	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FMT_SMF_EXT.3: Specification of Management Functions	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FMT_UNR_EXT.1: User Unenrollment Prevention	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target

The following table lists the TOE or Platform Security Functional Requirements. Note that the ST author will always include both FAU_GEN.1.1(2) and FAU_GEN.1.2(2) regardless; the only difference is whether FAU_GEN.1.2(2) is performed by the TOE or if the TSF relies on the underlying platform.

Table 7: TOE or Platform Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1(2): Audit Data Generation	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target

There are currently no "**Optional**" requirements.

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
n/a	n/a	n/a

There are currently no “**Selection-Based**” requirements.

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
n/a	n/a	n/a

The following table contains the “**Objective**” requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are not currently mandated by the EP but specify security functionality that is desirable, and are expected to transition from objective requirements to baseline requirements in future versions of the EP.

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG_EXT.1: Security Audit Event Storage	
FPT: Protection of the TSF	FPT_NET_EXT.1: Network Reachability	

6 Assurance Requirements

The following are the assurance requirements contained in the EPMDMA30:

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ASE_ECD.1: Extended Components Definition	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ASE_INT.1: ST Introduction	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ASE_REQ.1: Stated Security Requirements	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target

	ASE_SPD.1: Security Problem Definition	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ASE_TSS.1: TOE Summary Specification	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
ADV: Development	ADV_FSP.1 Basic Functional Specification	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	AGD_PRE.1: Preparative Procedures	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ALC_CMS.1: TOE CM Coverage	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
	ALC_TSU_EXT: Timely Security Updates	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target

7 Results of the evaluation

Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 11: Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
APE_ECD.1	Pass	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
APE_INT.1	Pass	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target
APE_OBJ.2	Pass	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target

APE_REQ.1	Pass	Apple iOS 10.2 (EPMDMA30/WLANCEP10) Security Target

8 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 as interpreted by the supplemental guidance in the EPMDMA Assurance Activities to determine whether or not the claims made are justified.
- **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.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5] atsec information security corporation, *Assurance Activity Report for Apple iOS 10.2 with MDM Agent and WLAN CLI*, Version 4.0, July 28, 2017.

[6] atsec information security corporation, *Apple iOS 10.2 Protection Profile Mobile Device Fundamentals, Extended Package for Mobile Device Management Agents, The General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package Wireless Local Area Network Clients Security Target,* Version 2.0, July 27, 2017.

[7] *Extended Package for Mobile Device Management Agents*, Version 3.0, 21 November 2016