National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients,

Version 1.0, February 8, 2016

Report Number:	**CCEVS-VR-PP-0036**
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 1
2 Identification 1
3 WLANCEP Description 2
4 Security Problem Description and Objectives 3
4.1 Assumptions 3
4.2 Threats 3
4.3 Organizational Security Policies 3
4.4 Security Objectives 3
5 Requirements 4
6 Assurance Requirements 6
7 Results of the evaluation 6
8 Glossary 6
9 Bibliography 7

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 the Wireless Local Area Network Clients Extended Package (version 1.0), also referred to as WLANCEP10. It presents a summary of the WLANCEP10 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the WLANCEP10 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 with MDM Agent and WLAN Client. The evaluation was performed by the atsec information security corporation Common Criteria Testing Laboratory (CCTL) in Austin, Texas, United States of America, and was completed in July 2017. This evaluation addressed the base requirements of the WLANCEP10, as well one of the additional requirements contained in Appendix B.

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 WLANCEP v.1.0 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 WLANCEP10, 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 WLANCEP10 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 WLANCEP10 was performed concurrent with the first product evaluation against the EP. In this case the TOE for this first product was the Apple iOS 10.2 with MDM Agent and WLAN CLI. The evaluation was performed by the astec information security corporation Common Criteria Testing Laboratory (CCTL) in Austin, Texas, United States of America, and was completed in July 2017.

The WLANCEP10 contains a set of "base" requirements that all conformant STs must include, and in addition, contains "Optional" and "Selection-based" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

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 WLANCEP10 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 WLANCEP10.

Protection Profile	*Wireless Local Area Network Clients Extended Package, Version 1.0, 8 February 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 Conformant
CCTL	atsec information security Corp. Austin, TX. USA
CCEVS Validators	Patrick Mallett, MITRE
	Kenneth Stutterheim, The Aerospace Corporation

3 WLANCEP Description

The WLANCEP10 is an Extended Package (EP) that describes security requirements for commercial off-the-shelf (COTS) Wireless Local Area Network (WLAN) Clients for the protection of data on a wireless network. A TOE defined by this EP is intended to be evaluated alongside a mobile device or desktop operating system and so it is defined as an EP of both the Mobile Device Fundamentals PP (MDF PP) and the General Purpose Operating Systems PP (GPOS PP). Compliant TOEs will provide essential services, such as cryptographic services, port access authentication, cryptographic functional testing, wireless network access, and trusted channel communication. Additional security features such as certificate authentication and storage are used in order to authenticate TLS implementation.

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.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

The threats listed below are addressed by WLAN Clients. Note that these threats are in addition to those defined in the base PPs, all of which apply to WLAN Clients.

Table 2: Threats

Threat Name	Threat Definition
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to WLAN Clients. However, all the organizational security policies in the base PPs apply to WLAN Clients.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.AUTH_COMM	The TOE will provide a means to ensure that it is communicating with an authorized Access Point and not some other entity pretending to be an authorized Access

TOE Security Obj.	TOE Security Objective Definition
	Point, and will provide assurance to the Access Point of its identity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide or use cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the TOE and its host environment.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.WIRELESS_ACCESS_POINT_CONNECTION	The TOE will provide the capability to restrict the wireless access points to which it will connect.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Requirements

As indicated above, requirements in the WLANCEP10 are comprised of the “**Base**” requirements and additional requirements that are conditionally optional. The following are table contains the “base” requirements that were validated as part of the Apple iOS 10.2 with MDM Agent and WLAN CLI evaluation activity referenced above.

Table 5: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FCS: Cryptographic Support	FCS_CKM.1/WLAN Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FCS_CKM.2/WLAN Cryptographic Key Distribution (GTK)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
	FCS_TLSC_EXT.1/WLAN Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FIA: Identification and Authentication	FIA_PAE_EXT.1 Port Access Entity Authentication	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FIA_X509_EXT.2/WLAN X.509 Certificate Authentication (EAP-TLS)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FMT: Security Management	FMT_SMF_EXT.1/WLAN Specification of Management Functions (Wireless LAN)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FPT: Protection of the TSF	FPT_TST_EXT.1/WLAN TSF Cryptographic Functionality Testing (Wireless LAN)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FTA: TOE Access	FTA_ WSE_EXT.1 Wireless Network Access	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
FTP: Trusted Path/Channels	FTP_ITC_EXT.1/WLAN Trusted Channel Communication (Wireless LAN)	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target

In addition to the mandatory requirements that will always be applicable to the TOE, there are different functional claims that must be made depending on which base PP the TOE claims. If this EP is used to extend the GPOS PP, the following additional SFR claim is needed:

Table 6: TOE Security Functional Requirements (GPOS PP Base)

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.3 Cryptographic Key Destruction	

Note that the Apple iOS 10.2 TOE claimed conformance to the MDF PP, so this SFR was not claimed in that evaluation.

The following table contains the "**Optional**" requirements contained in Appendix B, 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 included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_X509_EXT.4/Certificate Storage and Management	

The following table contains the "**Selection-Based**" 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 included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_TLSC_EXT.2/WLAN TLS Client Protocol	

There are no “**Objective**” requirements defined for this EP.

6 Assurance Requirements

This EP does not define any Security Assurance Requirements beyond those defined within the “base” requirements to which it can claim conformance.

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.

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
APE_ECD.1	Pass	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
APE_INT.1	Pass	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
APE_OBJ.2	Pass	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ WLANCEP10) Security Target
APE_REQ.1	Pass	Apple iOS 10.2 with MDM Agent and WLAN CLI (WLANCEP10/ 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 WLANCEP 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] *Wireless Local Area Network Clients Extended Package,* Version 1.0, 8 February 2016