National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Apple iOS 9.2 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor

Report Number: CCEVS-VR-10714-2016

Dated: March 10, 2016

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

Validation Team

Patrick Mallett, PhD

Ken Stutterheim

Common Criteria Testing Laboratory

W. Dean Freeman, CISSP

Anthony Busciglio

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Apple iOS 9.2 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in March 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security as summarized in the Apple IOS VPN Client Assurance Activity Report, Version 1.0. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2014 [VPNPP].

The Target of Evaluation (TOE) 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), as interpreted by the Assurance Activities contained in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013. 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 and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

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

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 Compliance List.

Table 1 provides information needed to completely identify the product, including:

- 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(s) 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 iOS 9.2 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
Security Target	Apple IOS VPN Client Security Target Security Target
Evaluation Technical Report	VID 10714 Common Criteria VPNPP Assurance Activity Report, version 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Apple Inc.
Developer	Apple Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Patrick Mallett, Ken Stutterheim

Table 1 Identification

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is a VPN client on a mobile operating system. The TOE is the VPN Client software only. The Apple iOS operating system has been separately validated (VID10695). The mobile operating system and hardware platforms are part of the TOE environment. When deployed, the TOE provides a tunnel to a VPN Gateway. The evaluated version of the TOE is version 9.2.

The Operating System on which the TOE is running is Apple iOS version 9.2. This is the same version of iOS which has undergone Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals Version 2.0. Each TOE platform contains two cryptographic modules; the Apple iOS CoreCrypto Kernel Module v6.0 and the Apple iOS CoreCrypto Module v6.0. These provide all TOE required cryptographic services.

Note: The TOE is the VPN Client software only. The Apple iOS operating system has been separately validated (VID10695).

4 Security Policy

The TOE is comprised of several security features, as identified below.

- Cryptography Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

The TOE provides the security functionality required by [VPNPP].

4.1 Cryptographic Support

The TOE provides IPsec VPN functionality for clients wishing to securely communicate with remote parties over unsecured networks. The TOE supports IPsec sessions established using IKEv2. The VPN tunnels are configured and controlled by Network Extension Framework, which is a part of the host operating system's Core OS Layer.

Each TOE platform contains two cryptographic modules; the Apple iOS CoreCrypto Kernel Module v6.0 and the Apple iOS CoreCrypto Module v6.0. These provide all TOE required cryptographic services including cryptographic key generation, key storage, AES encryption and decryption, cryptographic signature services, cryptographic hashing, keyed-hash message authentication and random bit generation. The CAVP algorithm certificates for each algorithm can be found in the table below.

Algorithm	Apple iOS CoreCrypto Kernel Module	Apple iOS CoreCrypto Module
AES	Certificate #3745, 3744, 3743	Certificate #3723, 3721, 3719
SHS	Certificate #3103, 3102, 3100	Certificate #3021, 3020, 3019
HMAC	Certificate #2449, 2448, 2447	Certificate #2435, 2434, 2432
RSA	Certificate #1925, 1924, 1923,	Certificate #1911, 1910, 1908
ECDSA	Certificate #798, 797, 796	Certificate #784, 783, 781
DRBG	Certificate #1024, 1023, 1022	Certificate #1011, 1010, 1008
NIST SP 800-56A CVL	N/A	Certificate #690, 689, 687

Table 2 CAVP Algorithm Certificates

4.2 User Data Protection

The TOE zeroizes all memory used to store packet contents upon reallocation for another purpose.

4.3 Identification and Authentication

All validation of X.509 certificates is performed by the iOS platform that the TOE is running on.

4.4 Security Management

The TOE provides the ability to manage all security functionality required by the Protection Profile via the use of configuration files (profiles).

4.5 Protection of the TSF

The TOE platform performs cryptographic self-tests at startup which ensures the TOE's ability to properly operate. The TOE platform also verifies all software updates via digital signature.

4.6 Trusted Path/Channels

The TOE is an IPsec VPN client. The TOE has the ability to establish IKEv2/IPsec protected communications with VPN gateways.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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.

Assumption	Assumption Definition
A.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

Table 3 Assumptions

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
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.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

Table 4 Threats

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 [VPNPP].
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Apple IOS VPN Client Security Target [ST], version 1.0;
- Apple iOS VPN Client Guidance Documentation [AGD], version 1.0

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a VPN client on a mobile operating system. The TOE is the VPN Client software only. The Apple iOS operating system has been separately validated (VID10695). The mobile operating system and hardware platforms are part of the TOE environment. When deployed, the TOE provides a tunnel to a VPN Gateway. The evaluated version of the TOE is version 9.2.

As evaluated, the TOE software runs on the following devices,

Device	Model	Operating System	Processor
iPhone 6	A1522 (GSM) A1522 (CDMA) A1524	Apple iOS9.2	Apple A8
iPhone 6 Plus	A1549 (GSM) A1549 (CDMA) A1586	Apple iOS9.2	Apple A8
iPhone 5s	A1533 (GSM) A1533 (CDMA) A1453 A1457 A1530	Apple iOS9.2	Apple A7
iPad mini 3	WiFi only WiFi + cellular	Apple iOS9.2	Apple A7
iPad Air 2	WiFi only WiFi + cellular	Apple iOS9.2	Apple A8X
iPad mini 2	WiFi only WiFi + cellular	Apple iOS9.2	Apple A7
iPad Air	WiFi only WiFi + cellular	Apple iOS9.2	Apple A7

Table 5 Hardware Devices

In the evaluated configuration, the device must be "supervised" and enrolled to an MDM platform capable of configuring and publishing the necessary Configuration Profile payload to the device.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for the Apple iOS 9.2 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor, which is not publically available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 [VPNPP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here.

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR) and summarized in the Apple IOS VPN Client Assurance Activity Report, Version 1.0. The reader of this document can assume that activities and work units received a passing 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 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Apple iOS 9.2 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the VPNPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. 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 VPN Client on iPhone and iPad devices using the A7 or A8/A8X processor that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 [VPNPP].

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 that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the VPNPP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the VPNPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team found that the TOE was identified. Additionally, the team verified that both the TOE and its supporting documentation are consistently reference the same version and use the same nomenclature. The evaluation team also verified that the vendor website identified the TOE version accurately.

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 that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team ran the set of tests specified by the Assurance Activities in the VPNPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the VPNPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator 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 addressed the vulnerability analysis Assurance Activities in the VPNPP, 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 test activities 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 performed the Assurance Activities in the VPNPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that the consumer pay special attention to the evaluated configuration of the device(s) and the specific functionality defined within the Security Target. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the security functional requirements within the Security Target was evaluated. Other functionality included in the product was not assessed as part of this evaluation.

The product contains more functionality than was covered by the evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

During evaluation several vulnerabilities were identified in the evaluated version of the TOE platform (outside of the TOE boundary). These vulnerabilities were addressed in iOS version 9.2.1. Per Policy Letter #22, TOE administrators are encouraged to deploy the latest patched version of the evaluated Operating System.

Note that the evaluated configuration is dependent upon the device being managed with a mobile device management solution.

11 Annexes

Not applicable.

12 Security Target

Please see the Apple IOS VPN Client Security Target [ST], version 1.0 March 2016.

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Apple IOS VPN Client Security Target [ST], version 1.0 March 2016
6. Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
7. Apple IOS VPN Client Assurance Activity Report, Version 1.0
8. Apple iOS VPN Client Guidance Documentation, March 2016, Version 1.0