National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Apple iOS 12 Contacts on iPhone and iPad

Report Number:	**CCEVS-VR-VID10961**
Dated:	**February 28, 2019**
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.

The MITRE Corporation

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Danielle F Canoles

Rutwij Kulkarni

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 12 Contacts on iPhone and iPad 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 February 2019. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security as summarized in the Apple iOS 12 Contacts Assurance Activity Report. 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 Application Software, version 1.2, dated, 22 April 2016 [SWAPP].

The Target of Evaluation 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 Application Software, version 1.2, dated, 22 April 2016 [SWAPP] and all applicable NIAP technical decisions for the technology. 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 and Technology 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 Profiles containing Assurance Activities, which are interpretations 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.

The target of evaluation is the Apple iOS 12 Contacts on iPhone and iPad and the associated TOE guidance documentation.

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.

Table 1 - Identification

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iOS 12 Contacts on iPhone and iPad
Protection Profile	Protection Profile for Application Software, version 1.2, dated, 22 April 2016
Security Target	Apple iOS 12 Contacts on iPhone and iPad Security Target Version 1.1
Evaluation Technical Report	VID10961 Assurance Activity Report, version 1.3
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Apple Inc.
Developer	Apple Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security, LLC
CCEVS Validators	Patrick Mallet, PhD., Kenneth Stutterheim

3 Architectural Information

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

The TOE is the Apple iOS 12 Contacts on iPhone and iPad application which runs on iPad and iPhone mobile devices. The product provides access and management of user contact information within the devices. The TOE is the Contacts application software only. The Apple iOS operating system has been separately validated as VID 10937. The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 12.

4 Security Policy

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

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

The TOE provides the security functionality as required by [SWAPP].

4.1 Cryptographic Support

The iOS platform provides HTTPS/TLS functionality to securely communicate with trusted entities. The TOE does not directly perform any cryptographic functions.

4.2 User Data Protection

The TOE requests no hardware or software resources during the use of the application. The TOE requires network access.

4.3 Identification and Authentication

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

4.4 Security Management

The TOE is installed completely pre-configured. No security related configuration is required for operation.

4.5 Privacy

The TOE will transmit contact information at the request of the user. The TOE provides a notification when sharing this information.

4.6 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 verifies all software updates via digital signature

4.7 Trusted Path/Channels

The TOE is a software application. The TOE has the ability to establish protected communications.

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.

Table 2 - Assumptions

Assumption	Assumption Definition
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

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.

Table 3 - Threats

Threat	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

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 Application Software, version 1.2, dated, 22 April 2016 [SWAPP].
- 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 PP and applicable Technical Decisions. Any additional security related functional capabilities that may be 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 12 Contacts Security Target, Version 1.1 [ST]
- Apple iOS 12 Contacts on iPhone and iPad Common Criteria Configuration Guide, Version 1.1, [AGD]

To use the product in the evaluated configuration, the product must be configured as specified in those guides. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device in its evaluated configuration. Consumers are encouraged to download the CC configuration guides directly from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a software application running on a mobile device (as listed below). The mobile device platform provides a host Operating System, controls that limit application behavior, and wireless connectivity. The Apple iOS 12 operating system has been separately validated. The TOE is the Contacts application only. The Apple iOS operating system has been separately validated (VID 10937). The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 12.

The Operating System on which the TOE is running is Apple iOS version 12. This is the same version of iOS which has undergone Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals Version 3.1.

As evaluated, the TOE Contacts software runs on the following devices running Apple iOS12:

Table 4 Hardware Devices

Device Name	Model	Processor	WiFi	Bluetooth
iPhone XS	A1920 A2097 A2098 A2099 A2100	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XS Max	A1921 A2101 A2102 A2103 A2104	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984 A2105 A2106 A2107 A2108	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone X	A1901 A1902 A1865	A11	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	5.0
iPhone 8 Plus/ iPhone 8	A1864, A1897, A1898, A1899/ A1863, A1905, A1906, A1907	A11	802.11a/b/g/n/ac 802.11a/b/g/n/ac	5.0
iPhone 7 Plus/ iPhone 7	A1661, A1784, A1785, A1786/ A1660, A1778, A1779, A1780	A10	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPhone 6S Plus/ iPhone 6S	A1634, A1687, A1690, A1699/ A1633, A1688, A1691, A1700	A9	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPhone SE	A1662 A1723 A1724	A9	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2
iPhone 6 Plus/ iPhone 6	A1522, A1524, A1593/ A1549, A1586, A1589	A8	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.0 4.0 4.0
iPad mini 4	A1538 A1550	A8	802.11a/b/g/n 802.11a/b/g/n	4.2 4.2

Device Name	Model	Processor	WiFi	Bluetooth
iPad Air 2	A1566 A1567	A8X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad (5th gen)	A1822 A1823	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 12.9” (1st Gen)	A1584 A1652	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 9.7”	A1673 A1674	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 12.9” (2nd Gen)	A1670 A1671	A10X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 10.5”	A1701 A1709	A10X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad 9.7”	A1893 A1954	A10	802.11a/b/g/n/ac	4.2

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 12 Contacts on iPhone and iPad, which is not publicly 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 Application Software, version 1.2, dated, 22 April 2016 [SWAPP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. Multiple test beds were constructed to exercise Application Software capabilities and claimed security functionality. The following tooling was used as part of the test activities,

- nmap version 7.70
- Wireshark 2.6.1
- SSH version OpenSSH_7.6p1
- QuickTime Player (for Video Recording) version 10.4 [Platform: MAC]
- Custom Script - "shasumfiles.sh" for FPT_TUD_EXT.1.1 Test#1

Note that platform based requirements testing leveraged the testing that had been previously vetted and approved as part of VID10937. Those VID10937 iOS 12 tests were run against the same models and processors as noted above.

8.3 TOE and Platform Testing Timeframe and Location

- The TOE specific testing was conducted during the timeframe of October 2018 through January 2019.
- The TOE specific testing was conducted by the Acumen Security CCTL located at Rockville, MD and Apple Inc. Reston facilities located at Reston, VA.
- Platform testing was conducted September 17-21, 2018 as part of VID10937 iOS 12 evaluation at Apple Inc. headquarters in Cupertino, CA.

8.4 Debug Version

- TOE testing was conducted on vendor provided debug version of the mobile device.

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 as summarized in the Apple iOS 12 Contacts Assurance Activity Report, Version 1.3. 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 12 Contacts on iPhone and iPad to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the SWAPP.

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 12 Contacts on iPhone and iPad 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 Application Software, version 1.2, dated 22 April 2016 [SWAPP].

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 SWAPP 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 SWAPP 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 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 SWAPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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 SWAPP, 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 following sources of public vulnerability information were searched on January 25, 2019:

- http://nvd.nist.gov
- http://www.us-cert.gov
- http://www.securityfocus.com
- http://cve.mitre.org

The search terms used included:

- iOS
- Apple
- Contacts
- iPhone
- iPad
- CoreCrypto

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 addressed the vulnerability analysis Assurance Activities in the SWAPP, 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 SWAPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

<NONE>

11 Annexes

Not applicable.

12 Security Target

Please see the Apple iOS 12 Contacts Security Target, Version 1.1 [ST].

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 12 Contacts Security Target, Version 1.1 [ST]
6. Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP]
7. Common Criteria SWAPP Assurance Activity Report, Apple iOS 12 Contacts, version 1.3, [AAR]
8. Apple iOS 12 Contacts on iPhone and iPad Common Criteria Configuration Guide, version 1.1 [AGD]