National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Apple iOS 14 and iPadOS 14: Contacts

Report Number: CCEVS-VR-VID11191-2021

Dated: August 20, 2021

Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D.

Jerome Myers, Ph.D.

DeRon Graves

Seada Mohammed

J David D Thompson

The Aerospace Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Thibaut Marconnet

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 14 and iPadOS 14: Contacts 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 August 2021. 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 14 and iPadOS 14: Contacts Assurance Activity Report (AAR). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [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 AAR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the 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 (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 Profiles (PPs) containing Evaluation 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 Compliant List.

The TOE is Apple iOS 14 and iPadOS 14: Contacts and the associated TOE guidance documentation.

Table 1 provides the 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 14 and iPadOS 14: Contacts
Protection Profile	Protection Profile for Application Software, Version 1.3, dated 01 March 2019
Security Target	Apple iOS 14 and iPadOS 14: Contacts Security Target, Version 1.1
Evaluation Technical Report	Apple iOS 14 and iPadOS 14: Contacts Assurance Activity Report, Version 1.1
CC Version	Version 3.1, Revision 5
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 Mallett, Ph.D. Jerome Myers, Ph.D. DeRon Graves Seada Mohammed J David D Thompson

3 Architectural Information

The TOE is the Apple Contacts application running on Apple iOS 14 and iPadOS 14. Contacts allows a user to access and edit contacts from personal, business, and other accounts.

Contacts is a first-party app, distributed with the operating system of the iPhone and iPad devices. Users can add contacts manually and/or they can be synchronized with an external server.

Note: The TOE is the Contacts application software only. The Apple iOS and iPadOS operating systems have been separately validated by NIAP.

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 required by the Protection Profile for Application Software Version 1.3 (PP_APP_v1.3).

4.1 Cryptographic Support

The TOE 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

The TOE uses platform-provided X.509 certificate validation functions to verify the validity and revocation status of HTTPS/TLS server certificates.

4.4 Security Management

The TOE does not provide management functionality. All management of settings is performed by the underlying platform. The TOE reads the platform-configured settings.

4.5 Privacy

The TOE does not request any personally identifiable information (PII) with the intent to transmit the data over the network. However, the TOE will transmit contact information at the request of the user.

4.6 Protection of the TSF

The TOE platform performs cryptographic self-tests at startup to ensure the TOE can properly operate. The TOE platform also 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 using platform-provided TLS/HTTPS.

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

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock 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 in compliance with 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

ID	Threat
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 1.3, dated 01 March 2019 [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 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 14 and iPadOS 14: Contacts Common Criteria Configuration Guide, Version 1.2 [AGD]

Any additional customer documentation provided with the product or available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is the Apple iOS 14 and iPadOS 14 Contacts application only, when configured in accordance with the documentation specified in Section 6. The Apple iOS and iPadOS operating systems have been separately validated against the Protection Profile for Mobile Device Fundamentals Version 3.1. The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 14.2.

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

Table 4 - Hardware Platforms

Device Name	Model	OS	Processor
iPhone 12 Pro Max	A2342 A2410 A2411 A2412	iOS	Apple A14 Bionic
iPhone 12 Pro	A2341 A2406 A2407 A2408	iOS	Apple A14 Bionic
iPhone 12	A2172 A2402 A2403 A2404	iOS	Apple A14 Bionic
iPhone 12 mini	A2176 A2398 A2399 A2400	iOS	Apple A14 Bionic
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	Apple A13 Bionic
iPhone 11 Pro	A2160 A2215 A2217	iOS	Apple A13 Bionic
iPhone 11	A2111 A2221 A2223	iOS	Apple A13 Bionic
iPhone SE (2nd generation)	A2275 A2296 A2298	iOS	Apple A13 Bionic
iPhone Xs Max	A1921 A2101 A2102 A2104	iOS	Apple A12 Bionic

Device Name	Model	OS	Processor
iPhone XS	A1920 A2097 A2098 A2099 A2100	iOS	Apple A12 Bionic
iPhone XR	A1984 A2105 A2106 A2107 A2108	iOS	Apple A12 Bionic
iPhone X	A1865 A1901 A1902	iOS	Apple A11 Bionic
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	Apple A11 Bionic
iPhone 8	A1863 A1905 A1906 A1907	iOS	Apple A11 Bionic
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	Apple A10 Fusion
iPhone 7	A1660 A1778 A1779 A1780	iOS	Apple A10 Fusion
iPhone 6s Plus	A1634 A1687 A1690 A1699	iOS	Apple A9
iPhone 6s	A1633 A1688 A1691 A1700	iOS	Apple A9
iPhone SE	A1662 A1723 A1724	iOS	Apple A9
iPad Air (4th generation)	A2316 A2324 A2072 A2325	iPadOS	Apple A14 Bionic

Device Name	Model	OS	Processor
iPad Pro 12.9-inch (4th generation)	A2229 A2232 A2069 A2233	iPadOS	Apple A12Z Bionic
iPad Pro 11-inch (2nd generation)	A2228 A2068 A2230 A2331	iPadOS	Apple A12Z Bionic
iPad Pro 12.9-inch (3rd generation)	A1876 A1895 A1983 A2014	iPadOS	Apple A12X Bionic
iPad Pro 11-inch (1st generation)	A1980 A1934 A1979 A2013	iPadOS	Apple A12X Bionic
iPad (8th generation)	A2270 A2428 A2429 A2430	iPadOS	Apple A12 Bionic
iPad Air (3rd generation)	A2123 A2152 A2153 A2154	iPadOS	Apple A12 Bionic
iPad mini (5th generation)	A2124 A2125 A2126 A2133	iPadOS	Apple A12 Bionic
iPad Pro (12.9-inch) (2nd generation)	A1670 A1671 A1821	iPadOS	Apple A10X Fusion
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	Apple A10X Fusion
iPad (7th generation)	A2198 A2199 A2200	iPadOS	Apple A10 Fusion
iPad (6th generation)	A1893 A1954	iPadOS	Apple A10 Fusion
iPad Pro (12.9-inch)	A1584 A1652	iPadOS	Apple A9X
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	Apple A9X
iPad (5th generation)	A1822 A1823	iPadOS	Apple A9

Table 5 - IT Environment Components

Component	Description
Hardware Platform	See the table above
Operating System	Apple iOS 14.2 or Apple iPadOS 14.2
Remote Server (optional)	Server for storing and synchronizing contacts

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the test reports for Apple iOS 14 and iPadOS 14: Contacts, which are not publicly available. The Section 4 of 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 1.3, dated 01 March 2019 [SWAPP]. The Independent Testing activity is documented in Section 4 of 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:

- tcpdump v4.9.3
- Quicktime Player v10.5
- Wireshark v3.2.2
- XCA 2.4
- nmap 7.91
- Baikal 0.8
- X509-MOD
- acumen-tlsc
- OpenSSL OCSP (v.1.1.1)
- Terminal 2.11
- ssh (OpenSSH_8.1p1, LibreSSL 2.7.3))
- iOS menu
- iOS Toolbox v1.3.14
- iRemoteX 1.0

8.3 TOE Testing Timeframe and Location

The TOE specific testing was conducted during the timeframe of December 2020 to July 2021.

The TOE specific testing was conducted at Acumen Security CCTL located at Rockville, MD and Apple Inc. headquarters in Cupertino, CA.

The testing performed at Apple Inc. was performed by the vendor and witnessed by the CCTL. All configurations were verified by the CCTL prior to each session. Test evidence was uploaded via a secure site with a controlled and limited access to the involved lab and vendor personnel. All evidence used were saved and verified by the CCTL.

8.4 Debug Version

The devices used for remote testing (testing performed at Apple Inc.) used a proprietary build of the platform OS that would allow additional debugging and filesystem access without modifying the TOE.

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 14 and iPadOS 14: Contacts AAR. 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 5 and CEM version 3.1 rev 5. The evaluation determined Apple iOS 14 and iPadOS 14: Contacts is 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 the 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 Apple iOS 14 and iPadOS 14: Contacts 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 1.3, dated 01 March 2019 [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 ST'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 Evaluation Activities in the SWAPP and recorded the results in the test reports. The results are summarized in the ETR and AAR.

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 public search for vulnerabilities was performed on July 8, 2021.

The National Vulnerability Database (NVD) was searched for publicly reported CVEs.

The TOE, underlying platform OS, and all platform libraries/frameworks are distributed together, and vulnerabilities are reported under the platform OS CPE. The following CPEs were searched:

- cpe:2.3:o:apple:ipados:14.2:*:*:*:*:*:*:*
- cpe:2.3:o:apple:iphone_os:14.2:*:*:*:*:*:*:*

No publicly known vulnerabilities were discovered in the TOE.

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

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Apple iOS 14 and iPadOS 14: Contacts Common Criteria Configuration Guide, Version 1.2, August 2021 document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness..

11 Annexes

Not applicable.

12 Security Target

Please see the Apple iOS 14 and iPadOS 14: Contacts Security Target, Version 1.2, August 2021. [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 5
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5
5. Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP]
6. Apple iOS 14 and iPadOS 14: Contacts Security Target, Version 1.2, August 2021. [ST]
7. Apple iOS 14 and iPadOS 14: Contacts Security Target addendum, Version 1.0, July 2021.
8. Apple iOS 14 and iPadOS 14: Contacts Assurance Activity Report, Version 1.2, August 2021. [AAR]
9. Apple iOS 14 and iPadOS 14: Contacts Common Criteria Configuration Guide, Version 1.2, August 2021. [AGD]