National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Apple iOS and iPadOS 13 Safari

Report Number:	**CCEVS-VR-VID11060-2020**
Dated:	**5 June 2020**
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

Sheldon Durrant
John Butterworth
Lisa Mitchell
Patrick Mallett PhD

The MITRE 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 and iPadOS 13 Safari 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 June 2020. 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 and iPadOS 13 Safari Assurance Activity Report. 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] and Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP].

The 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. 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 Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP] 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 (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 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.

The target of evaluation is the Apple iOS and iPadOS 13 Safari 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 results 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 and iPadOS 13 Safari
Protection Profile	Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP] Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP]
Security Target	Apple iOS and iPadOS 13 Safari Security Target Version 1.1
Evaluation Technical Report	Apple iOS and iPadOS 13 Safari Assurance Activity Report, Version 1.3
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	Sheldon Durrant John Butterworth Patrick Mallett

3 Architectural Information

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

The TOE is the Apple iOS and iPadOS Safari application which runs on iPad and iPhone devices. The product provides access to HTTPS/TLS connections via a browser for user connectivity.

Note: The TOE is the Safari software only. The Apple iOS and iPadOS operating systems are undergoing evaluation separately and will be posted to the Product Compliant List when successfully completed.

The TOE is an application on a mobile operating system. The Apple iOS and iPadOS operating systems are being 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 13.4.1.

4 Security Policy

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

- Cryptographic Support
- User Data Protection
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels

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

4.1 Cryptographic Support

The platform provides TLS/HTTPS connectivity for users attempting to communicate with secure URLs. The TOE does not directly perform any cryptographic functions. The TOE invokes the platform cryptography for secure credential storage.

4.2 User Data Protection

The TOE requests access to network connectivity, camera, microphone, location services, and address book, and communicates with the wireless network when invoked by the user. The TOE runs inside of a sandbox where each browser tab is isolated. In addition, the TOE supports blocking of third-party cookies. When a cookie has been set with the 'secure' attribute, the TOE will only send the cookie over HTTPS.

4.3 Security Management

The platform provides the ability to configure the TOE. No credentials are installed by default.

4.4 Privacy

If the user logs into iCloud Account on two or more devices, two devices within Bluetooth range of each other have the ability to automatically "continue" browsing with the same URL provided via iCloud.

The TOE does not specifically request PII from the user. Any information provided by the user is entered without prompting from the TOE.

4.5 Protection of the TSF

The TOE does not permit automatic downloads. All downloads are at the request of a user and require approval. The TOE does not support add-ons. The only supported mobile code is signed JavaScript. No third-party libraries are leveraged by the TOE. The TOE platform verifies all software updates via digital signature.

4.6 Trusted Path/Channels

The TOE is a software application. The TOE leverages the platform to establish HTTPS/TLS 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

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.
T.FLAWED_ADDON	Web browser functionality can be extended through the integration of third-party utilities and tools. Malicious or vulnerable add-ons could result in attacks against the system. Such attacks can allow unauthorized access to sensitive information in the browser, unauthorized access to the platform's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.
T.SAME-ORIGIN_VIOLATION	Violating the same-origin policy is a specialized type of network attack (covered generally as T.NETWORK_ATTACK in the App PP) which involves web content violating access control policies enforced by a web browser to separate the content of different web domains. It is specifically identified as a threat to web browsers, since they implement the access control policies that are violated in these attacks.

ID	Threat
	Attacks which involve same origin violations include: - Insufficient protection of session tokens can lead to session hijacking, where a token is captured and reused in order to gain the privileges of the user who initiated the session. - Cross-site scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks are methods used to compromise user credentials (usually by stealing the user's session token) to a web site. These attacks are more likely a result of server security problems, but some browsers incorporate technologies that try to detect the attacks. - Inadequate sandboxing of browser windows/tabs or a faulty cross domain communications model can lead to leakage of content from one domain in one window/tab to a different domain in a different window/tab. Such attacks leverage the ability of browsers to display content from multiple domains simultaneously.

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] and Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP].
- 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 and iPadOS 13 Safari Common Criteria Configuration Guide, Version 1.5 [AGD]

Any additional customer documentation provided with the product, or that is 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 an application on a mobile operating system. The TOE is the Safari browser application only. 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 13.4.1.

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

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11 Pro	A2160 A2215 A2216 A2217	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11	A2111 A2221 A2222 A2223	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone SE (2nd Gen)	A2275 A2296 A2298	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone Xs Max	A1921 A2101 A2102 A2103 A2104	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984 A2105 A2106 A2107 A2108	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone X	A1865 A1901 A1902 A1903	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8 Plus	A1864 A1897	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
	A1898 A1899				
iPhone 8	A1863 A1905 A1906 A1907	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 7	A1660 A1778 A1779 A1780	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 6S Plus	A1634 A1687 A1690 A1699	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone 6s	A1633 A1688 A1691 A1700	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone SE	A1662 A1723 A1724	iOS	A9	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (4th gen)	A2229 A2232 A2069 A2233	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 11” (2nd gen)	A2228 A2068 A2230 A2331	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 12.9-inch (3rd gen)	A1876 A1895 A1983 A2014	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Pro 11-inch	A1980 A1934 A1979 A2013	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Air (3rd gen)	A2123 A2152 A2153 A2154	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPad mini (5th gen)	A2124 A2125 A2126 A2133	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad Pro (12.9-inch 2nd Gen)	A1670 A1671 A1821	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad (7th gen)	A2197 A2198 A2199 A2200	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad (6th gen)	A1893 A1954	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (12.9)	A1584 A1652	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad (5th gen)	A1822 A1823	iPadOS	A9	802.11a/b/g/n/ac	4.2
iPad Air 2	A1566 A1567	iPadOS	A8X	802.11a/b/g/n/ac	4.2
iPad mini 4	A1538 A1550	iPadOS	A8	802.11a/b/g/n	4.2

Table 4 IT Environment Components

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 and iPadOS 13 Safari, 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 1.3, dated 01 March 2019 [SWAPP] and Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP]. 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:

- macOS Safari v13.0.5
- Wireshark v2.6.9
- OpenSSH v7.9p1
- QuickTime Player v10.15
- nmap v7.80

8.3 TOE Testing Timeframe and Location

- The TOE specific testing was conducted during the timeframe of October 2019 through June 2020.
- The TOE specific testing was conducted at Acumen Security CCTL located at Rockville, MD and Apple Inc. headquarters in Cupertino, CA.

8.4 Debug Version

- Testing was conducted on vendor provided mobile devices with developer access.

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 and iPadOS 13 Safari Assurance Activity Report. 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 the Apple iOS and iPadOS 13 Safari 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 and iPadOS 13 Safari 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] and Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP].

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

The following components of the TOE were searched:

Component	CPE
Apple iOS 13.4.1	cpe:2.3:*:apple:iphone_os:13.4.1:*:*:*:*:*:*:*
Apple iOS 13.4	cpe:2.3:*:apple:iphone_os:13.4:*:*:*:*:*:*:*
Apple iOS 13.3.1	cpe:2.3:*:apple:iphone_os:13.3.1:*:*:*:*:*:*:*
Apple iPadOS 13.4.1	cpe:2.3:*:apple:ipad_os:13.4.1:*:*:*:*:*:*:*

Apple iPadOS 13.4	cpe:2.3:*:apple:ipad_os:13.4:*:*:*:*:*:*:*
Apple iPadOS 13.3.1	cpe:2.3:*:apple:ipad_os:13.3.1:*:*:*:*:*:*:*

The TOE (Application), underlying platform OS, and all platform libraries/frameworks are distributed together, and vulnerabilities are reported under the platform OS CPE. CPEs for Apple Safari and Webkit were examined and determined to be for much older versions (e.g. iOS 9).

No publicly known vulnerabilities were discovered in the TOE version or the two prior versions.

The evaluator also scanned the TOE using McAfee Mobile Security: Privacy App v4.2

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 WEBBROWSEREP, 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 WEBBROWSEREP, 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 CC Guide 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.

11 Annexes

Not applicable.

12 Security Target

Please see the Apple iOS and iPadOS 13 Safari 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 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. Apple iOS and iPadOS 13 Safari Security Target, Version 1.1 [ST]
6. Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP]
7. Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP]
8. Apple iOS and iPadOS 13 Safari Assurance Activity Report, Version 1.3 [AAR]
9. Apple iOS and iPadOS 13 Safari Guidance Documentation, Version 1.5 [AGD]