Assurance Activity Report for Apple iOS 14 and iPadOS 14: Safari

Apple iOS 14 and iPadOS 14: Safari Security Target
Version 1.1

Application Software Protection Profile, version 1.3
Application Software Extended Package for Web Browsers, Version 2.0

AAR Version 1.1, August 2021

Evaluated by:

intertek
acumen
security

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

N I A P

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Apple Inc.

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Apple Inc.

Evaluation Personnel:
Kenji Yoshino
Thibaut Marconnet

Acumen Security, LLC

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	July 2021	Initial Release
1.1	August 2021	Updated to address ECR comments

Table of Contents

1 TOE Overview

The TOE is the Apple Safari application running on Apple iOS 14 and iPadOS 14. Safari is the default web browser on iPhone and iPad devices. Safari provides tracking and privacy protections while allowing the user to securely access HTTPS/TLS protected websites. Safari is a first party-app, distributed with the operating system of the iPhone and iPad devices.

1.1 TOE Description

This section provides a general description of the TOE, including physical boundaries, security functions, and relevant TOE documentation and references.

The TOE does not have a physical boundary because the TOE is a software application. As evaluated, the TOE runs on the following physical devices:

Table 1 – 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
iPad Pro 12.9-inch (4th generation)	A2229 A2232 A2069 A2233	iPadOS	Apple A12Z Bionic

Device Name	Model	OS	Processor
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

2 Security Functional Requirement Identification

The following table identifies each of SFRs included in this evaluation:

Table 2 – SFRs

Requirement	Description
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FDP_ACF_EXT.1	Local and Session Storage Separation
FDP_COO_EXT.1	Cookie Blocking
FDP_DAR_EXT.1	Encryption of Sensitive Application Data
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_SBX_EXT.1	Sandboxing of Rendering Processes
FDP_SOP_EXT.1	Same Origin Policy
FDP_STR_EXT.1	Secure Transmission of Cookie Data
FDP_TRK_EXT.1	Tracking Information Collection
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_MOF_EXT.1	Management of Functions Behavior
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_AON_EXT.1	Support for Only Trusted Add-ons
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_DNL_EXT.1	File Downloads
FPT_IDV_EXT.1	Software Identification and Versions
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_MCD_EXT.1	Mobile Code
FPT_TUD_EXT.1	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

3 Equivalency Analysis

The following equivalency analysis provides a per-category analysis of key areas of differentiation for the TOE. The areas examined will use the areas and analysis description provided in the supporting documentation for the Application Software PP.

Table 3 – Equivalency Analysis

Appendix E Section/Requirement	Rationale
E.3 Specific Guidance for Determining Product Model Equivalence	The TOE is only a single “model,” so no equivalency claim is necessary.
E.4 Specific Guidance for Determining Product Version Equivalence	The TOE is only a single version, so no equivalency claim is necessary.
E.5.2.1 Platform Equivalence—Hardware/Virtual Hardware Platforms	N/A: The TOE does not run on a virtual platform.
E.5.2 Platform Equivalence—OS Platforms: Platform Architectures	The TOE runs on a single processor architecture (ARM) and a single instruction set (A64), so the Platform Architecture is considered equivalent.
E.5.2 Platform Equivalence—OS Platforms: Platform Vendors	Apple is the sole vendor for the platforms, so the Platform Vendors are considered equivalent.
E.5.2 Platform Equivalence—OS Platforms: Platform Versions	The TOE runs on two OSs: iOS 14.6 and iPadOS 14.6.
E.5.2 Platform Equivalence—OS Platforms: Platform Interfaces	There are no differences in device interfaces and OS APIs that are relevant to the way the platform provides PP-specified security functionality to the TOE, so the Platform Interfaces are considered equivalent.
E.5.3 Software-based Execution Environment Platform Equivalence	N/A: The TOE does not run on a software-based execution environment.
E.6 Level of Specificity for Tested Configurations and Claimed Equivalent Configurations	The TOE is a Traditional Application using a single instruction set, identical device interfaces, and identical OS API invocation related to PP-specified security functionality.

Based on the above factors, Acumen Security tested the TOE on each OS and on each CPU architecture version.

Table 4 – Tested Devices

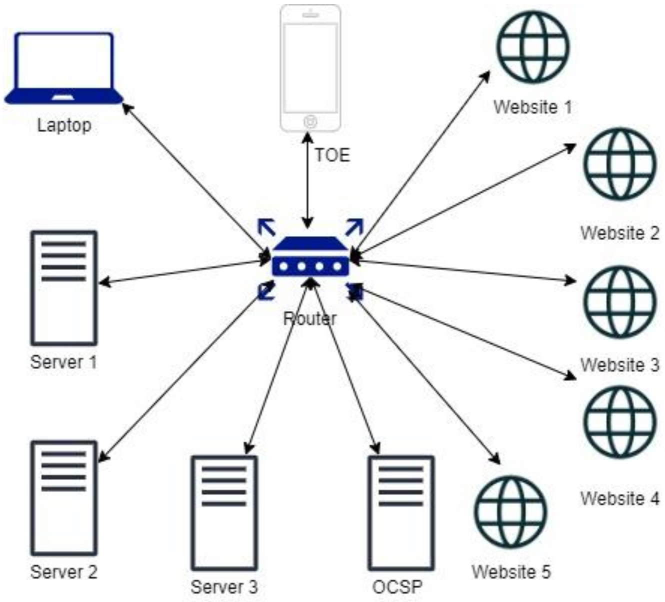
Device	CPU Model	Operating System
iPhone 6s	Apple A9	Apple iOS
iPhone XR	Apple A12 Bionic	Apple iOS
iPhone 11	Apple A13 Bionic	Apple iOS
iPhone 12	Apple A14 Bionic	Apple iOS
iPad Pro (10.5-inch)	Apple A10X Fusion	Apple iPadOS
iPad Pro 11-inch (1st generation)	Apple A12X Bionic	Apple iPadOS
iPad Air (4th generation)	Apple A14 Bionic	Apple iPadOS

4 Test Diagram

4.1 Testing Location

- Acumen Security, 2400 Research Boulevard, Suite 395, Rockville, MD 20850
- Apple, One Apple Parkway, Cupertino, CA 95014

4.2 Test Bed 1

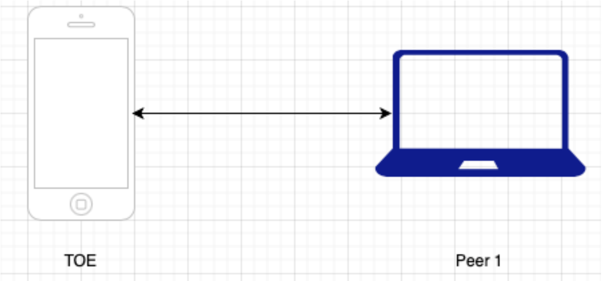


- TOE:
  - iOS/iPadOS: 14.6
  - Protocols: HTTPS/TLSv1.2
  - Time: Set with NTP and verified
- Router:
  - Model: Ubiquiti EdgeRouter X
  - Software: EdgeOS v2.0.9
  - Tools: tcpdump v4.9.3
- Laptop:
  - Model: MacBook Air 2020
  - Software Version: macOS Big Sur v11.2.2
  - Tools: Quicktime Player v10.5, Wireshark v3.2.2, nmap 7.91, XCA 2.4
  - Time: Set with NTP and verified
- Web Server 1:
  - Model: Virtual Machine running on Virtual Box 6.1
  - Software: Ubuntu 18.04 LTS
  - Name: iOSTestInstance
  - Protocols: HTTPS/TLSv1.2
  - Tools: Apache v2.4.29, OpenSSL 1.1.1 (11 September 2018), X509-MOD, acumen-tlsc
  - Time: Set with NTP and verified
- Web Server 2:

  - Model: Virtual Machine running on Virtual Box 6.1
  - Software: Ubuntu 18.04 LTS
  - Name: iOSTestInstance2
  - Protocols: HTTPS/TLSv1.2
  - Tools: Apache v2.4.29
  - Time: Set with NTP and verified
- OCSP:
  - Software: Ubuntu 18.04 LTS
  - Name: Ubuntu VM
  - Protocols: HTTPS/TLSv1.2
  - Tools: OpenSSL OCSP 1.1.1 (11 September 2018)
  - Time: Set with NTP and verified
- Website 1:
  - Domain name: tomshardware.com
  - Test: FDP_COO_EXT.1
  - Protocols: HTTPS/TLSv1.2
- Website 2:
  - Domain Name: maps.google.com
  - Test: FDP_TRK_EXT.1
  - Protocols: HTTPS/TLSv1.2
- Website 3:
  - Domain Name: security.stackexchange.com
  - Test: FTP_DIT_EXT.1.1
  - Protocols: HTTPS/TLSv1.2
- Website 4:
  - Domain Name: mail.google.com
  - Test: FCS_STO_EXT.1
  - Protocols: HTTPS
- Website 5:
  - Domain Name: adobe.com
  - Test: FDP_SBX_EXT.1.1
  - Protocols: HTTPS

4.3 Test Bed 2

The CCTL used a secure channel to remotely witness testing of the TOE performed by the vendor. All configurations were verified by the CCTL prior to each session. The devices used for remote testing used a proprietary build of the platform OS that would allow additional debugging and filesystem access without modifying the TOE. 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.



- TOE:

iOS/iPadOS: 14.2[1]

  -
  - Protocols: SSH
- Peer 1:
  - Model: MacBook Pro
  - Software version: macOS 11.2
  - Protocols: SSH
  - Tools:
    - Terminal 2.11 (Terminal sessions to DUT - ssh (OpenSSH_8.1p1, LibreSSL 2.7.3))
    - iOS menu (Menu option to ssh to DUT)
    - iOS Toolbox v1.3.14 (Tool for access to files, executables, multi services)
    - iRemoteX 1.0 (Remote control of Device via UI)

[1] During the course of the evaluation, the TOE was updated to version 14.6. Only architectural and build tests were run on version 14.2. The updates from 14.2 to 14.6 do not change the architecture or way the TOE is built, so the tests were not rerun on version 14.6.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Cryptographic Support)

5.1.1 FCS_RBG_EXT.1

5.1.1.1 FCS_RBG_EXT.1.1 TSS

Objective	If **use no DRBG functionality** is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.
Evaluator Findings	The evaluator found that the TSS in section 6 "TOE Summary Specification", specifically the FCS_RBG_EXT.1 entry of Table 13, states: "The TOE does not use DRBG functionality." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FCS_CKM_EXT.1

5.1.2.1 FCS_CKM_EXT.1.1 TSS

Objective	The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the **generate no asymmetric cryptographic keys** selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.
Evaluator Findings	The evaluator found that the TSS in section 6 "TOE Summary Specification", specifically the FCS_CKM_EXT.1 entry of Table 13, states: "The TOE does not generate asymmetric cryptographic keys. The asymmetric cryptographic key generation that is related to TOE operation is implemented by the platform within the platform provided cryptographic protocols." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FCS_STO_EXT.1

5.1.3.1 FCS_STO_EXT.1.1 TSS

Objective	The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.
Evaluator Findings	The evaluator checked the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. The TSS in section 6 "TOE Summary Specification" FCS_STO_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE allows the user to save usernames and passwords

	used to login to websites in the Keychain (i.e., platform provide credential store). Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (User Data Protection)

5.2.1 FDP_ACF_EXT.1

5.2.1.1 FDP_ACF_EXT.1.1 TSS

Objective	The evaluator shall examine the TSS to ensure it describes how the browser separates local and session storage.
Evaluator Findings	The evaluator examined the TSS in section 6 “TOE Summary Specification”, specifically the FDP_ACF_EXT.1 entry of Table 13, describes how the browser separates local and session storage. “The TOE utilizes the platform OS process separation to isolate ephemeral/session storage. Each tab is a separate process, so the process separation prevents tabs from accessing any resources loaded by a different tab.” “The main TOE process provides the persistent/local storage. When a tab loads information into local storage, it also copies the data along with the origin to the main process for persistence. The main process enforces the same origin policy when determining if the local storage data should be shared with any other tabs that share the same origin.” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FDP_ACF_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to verify that it documents the location on the file system that will be used for local storage and the location used for session storage.
Evaluator Findings	The evaluator examined the operational guidance to verify that it documents the location on the file system that will be used for local storage and the location used for session storage. Section 5.1, “Local and Session Storage Separation,” was used to determine the verdict of this activity. Upon investigation, the evaluator found that Session data is only stored in memory dedicated to the browser tab. Local storage data is only stored in the dedicated browser sandbox. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.3 FDP_COO_EXT.1

5.2.3.1 FDP_COO_EXT.1.1 TSS

Objective	The evaluator shall examine the TSS to ensure it describes how the browser blocks

	third party cookies and when the blocking occurs (e.g., automatically, when blocking is enabled).
Evaluator Findings	The evaluator examined the TSS in section 6 "TOE Summary Specification", specifically the FDP_COO_EXT.1 entry of Table 13, describes how the browser blocks third party cookies and when the blocking occurs. Upon investigation, the TOE can be configured through setting to block all cookies via communication with the underlying platforms settings menu. When configured, the TOE will reject any attempts from a website to use third-party cookies. Based on these findings, this assurance activity is considered satisfied.
Result	Pass

5.2.3.2 FDP_COO_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to verify that it provides a description of the configuration option for blocking of third party cookies.
Evaluator Findings	The evaluator examined the operational guidance to verify that it provides a description of the configuration option for blocking of third party cookies. Section 5.4, "Cookie Blocking, Tracking Behavior, and Other Security Features" of the AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that AGD states blocking third party cookies involve the following, • Tap Settings > Safari > Block All Cookies Based on these findings, this activity is considered satisfied.
Result	Pass

5.2.4 FDP_DEC_EXT.1

5.2.4.1 FDP_DEC_EXT.1.1 Guidance

Objective	The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator verified that either the application software or its documentation provides a list of the hardware resources it accesses. AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that section titled "Resource Usage" of the AGD identifies that the following hardware resources are accessed by the TOE: • Network Connectivity: This is required for Safari to facilitate communications with remote websites. • Camera: This is required when a website requests access to the device's camera input. • Microphone: This is required when a website requests access to the device's audio input. • Location Services: This required to share location with websites.

	This is consistent with the access described in ST. Based on these findings, this activity is considered satisfied.
Result	Pass

5.2.4.2 FDP_DEC_EXT.1.2 Guidance

Objective	The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator verified that either the application software or its documentation provides a list of the sensitive information repositories it accesses. AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that section titled “Resource Usage” of the AGD identifies that the following sensitive information repository is accessed by the TOE: • Keychain • Address Book This is consistent with the access described in ST. Additionally, the evaluator found that section 4 “Resource Usage” of the AGD provides a justification for why access to the Keychain is required. Based on these findings, this activity is considered satisfied.
Result	Pass

5.2.5 FDP_DAR_EXT.1

5.2.5.1 FDP_DAR_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS. If **not store any sensitive data** is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below.
Evaluator Findings	The evaluator inspected the TSS and ensured that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally. The TSS in section 6 “TOE Summary Specification” FDP_DAR_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that all user requested browser information (autofill information) is stored on the platform under Class A (Complete Protection). No other files are stored by the application. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.6 FDP_SBX_EXT.1

5.2.6.1 FDP_SBX_EXT.1.1 TSS

Objective	The evaluator shall examine the TSS to ensure it describes how the rendering of HTML and interpretation of JavaScript is performed by the browser in terms of the platform processes that are involved (with "process" being an active entity that executes code). For the processes that render HTML or interpret JavaScript, the evaluator shall examine the TSS to check that it describes how these processes are prevented from accessing the platform file system. The evaluator shall check the TSS to ensure it describes each platform-provided IPC mechanism, and details for each mechanism how the rendering process is unable to use it to communicate with non-browser processes. The evaluator shall also confirm that the TSS describes how IPC and file system access is enabled (if this capability is implemented); for instance, through a more privileged browser process that does not perform web page rendering. The evaluator shall ensure that these descriptions are present for all platforms claimed in the ST. For each additional mechanism listed in the third bullet of this component by the ST author, the evaluator shall examine the TSS to ensure 1) the mechanisms are described; 2) the description of the mechanisms are sufficiently detailed to determine that it contributes to the principle of least privilege being implemented in the rendering process; and 3) appropriate supporting information is provided in the TSS (or pointers to such information are provided) that provides context for understanding the claimed least privilege mechanisms.
Evaluator Findings	The evaluator examined the TSS in section 6 "TOE Summary Specification" FDP_SBX_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. The TSS states the "TOE is a first-party application provided as part of the underlying platform. When requests to render HTML or interpret JavaScript are done by a website, the TOE process itself will process the request underlying platform's libraries. The TOE runs in a dedicated sandbox environment on the platform. This completely isolates the requests from accessing the platform's file system. The TOE has no access to the underlying file system. This functionality is enabled by default with no user intervention required." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.6.2 FDP_SBX_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to determine that it provides a description of the restrictions available on rendering processes. Additionally, if such mechanisms are configurable (for instance, if a user can choose which mechanisms to "turn on"), the evaluator shall examine the operational guidance to ensure that the method for enabling and disabling the mechanisms are provided, and the consequences of such actions are described.
Evaluator Findings	The evaluator examined the operational guidance to determine that it provides a description of the restrictions available on rendering processes. Section 4.2, "Sandboxing of Rendering Processes," of the AGD was used to determine the

	verdict of this activity. Upon investigation, the evaluator found that the rendering process can only directly access the area of the file system dedicated to the browser. No other access is available. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.7 FDP_SOP_EXT.1

5.2.7.1 FDP_SOP_EXT.1.2 TSS

Objective	The evaluator shall examine the TSS to ensure it describes its implementation of a same origin policy and explains how it complies with RFC 6454. If the browser allows the relaxation of the same origin policy for subdomains in different windows/tabs, the TSS shall describe how these exceptions are implemented.
Evaluator Findings	The evaluator examined the TSS to ensure it describes its implementation of a same origin policy and explains how it complies with RFC 6454. The TSS in section 6 “TOE Summary Specification” FDP_SOP_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE is fully compliant with RFC 6454 in that the policy is applied to all web browser tab/windows independently, there is not situation where conformation is relaxed in anyway. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.8 FDP_STR_EXT.1

5.2.8.1 FDP_STR_EXT.1.1 TSS

Objective	The evaluator shall examine the TSS to verify it describes the browser's support for the "secure" attribute of the set-cookie header in accordance with RFC 6265, including the required sending of cookies containing this attribute over HTTPS.
Evaluator Findings	The evaluator examined the TSS to verify it describes the browser's support for the "secure" attribute of the set-cookie header in accordance with RFC 6265, including the required sending of cookies containing this attribute over HTTPS. The TSS in section 6 “TOE Summary Specification” FDP_STR_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that cookies that are sent over HTTPS are required to contain this attribute within the header. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.9 FDP_TRK_EXT.1

5.2.9.1 FDP_TRK_EXT.1.1 TSS

Objective	The evaluator shall examine the TSS to ensure it describes the browser's support for tracking information and specifies the tracking information that the browser allows websites to collect about the browser user.
Evaluator Findings	The evaluator examined the TSS to ensure it describes the browser's support

	for tracking information and specifies the tracking information that the browser allows websites to collect about the browser user. The TSS in section 6 "TOE Summary Specification" FDP_TRK_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the browser allows the tracking of geolocation information and browser preferences after the user accepts a notification from the browser. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.9.2 FDP_TRK_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to ensure it describes any notifications that the user will receive when tracking information is requested by a website and the options that the user has upon receiving the notification.
Evaluator Findings	The evaluator examined the operational guidance to ensure if it describes any notifications that the user will receive when tracking information is requested by a website and the options that the user has upon receiving the notification. Section 5.3, "Tracking Information Collection," of the AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that the browser provides a notification to the user whenever tracking information for geolocation or browser preferences is requested. Additionally, a visual example of this notification is provided. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (Identification and Authentication)

5.3.1 FIA_X509_EXT.1

5.3.1.1 FIA_X509_EXT.1.1 TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.
Evaluator Findings	The evaluator examined section 6 "TOE Summary Specification" FCS_STO_EXT.1 entry of Table 13 in the ST to verify that the TSS describes where the check of validity of the certificates takes place and the certificate path validation algorithm. Upon investigation, the evaluator found that the TSS states that, "X.509 certificates are validated during session establishment with an HTTPS/TLS server." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2 FIA_X509_EXT.2

5.3.2.1 FIA_X509_EXT.2.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the FIA_X509_EXT.1 entry of Table 13 in section 6 in the ST to verify that the TSS describes how the TOE chooses which certificates to use. Upon

	investigation, the evaluator found that the TSS states that, “The platform uses the certificates provided by the TLS server and the certificates in the local trust store to build the certificate chain.” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.2 FIA_X509_EXT.2.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described.
Evaluator Findings	The evaluator examined the FIA_X509_EXT.2 entry of Table 13 in section 6 in the ST to verify that the TSS describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that, “The certificate is accepted if its revocation status cannot be determined.” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.3 FIA_X509_EXT.2.1 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it describes configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled “Digital Certificates” in the AGD to verify that it describes configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD provides instructions for adding trust anchors. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.4 FIA_X509_EXT.2.1 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the FIA_X509_EXT.1 entry of Table 13 in section 6 in the ST and determined that the TOE always accepts certificates when the revocation status cannot be determined, so this evaluation activity is N/A.
Verdict	Pass

5.4 TSS and Guidance Activities (Security Management)

5.4.1 FMT_MEC_EXT.1

5.4.1.1 FMT_MEC_EXT.1.1 TSS (TD0437)

Objective	The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS

	shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.
Evaluator Findings	The evaluator examined the TSS in section 6 “TOE Summary Specification” FMT_MEC_EXT.1 entry in Table 13 of the ST to determine the TOE maintains a restricted configuration with no management functions being performed by users and all configuration options are set by the underlying platform. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

5.4.2 FMT_CFG_EXT.1

5.4.2.1 FMT_CFG_EXT.1.1 TSS

Objective	The evaluator shall check the TSS to determine if the application requires any type of credentials and if the applications installs with default credentials.
Evaluator Findings	The evaluator examined the TSS section 6 “TOE Summary Specification” FMT_CFG_EXT.1 entry in Table 13 of the ST to determine if the application requires any credentials and if it installs with default credentials. Section 6 of the ST was used to determine the verdict of this assurance activity. The evaluator found that the TOE does not come with any default credentials. The user must configure an account first before accessing the TOE and underlying platform. Based on this, the evaluation is considered satisfied.
Verdict	Pass

5.4.3 FMT_MOF_EXT.1

5.4.3.1 FMT_MOF_EXT.1.1 TSS

Objective	The evaluator shall verify that the TSS describes those management functions which may only be configured by the browser platform administrator and cannot be over-ridden by the user when set according to policy.
Evaluator Findings	The evaluator verified that the TSS in section 6 “TOE Summary Specification” FMT_MOF_EXT.1 entry of Table 13 of the ST describes those management functions which may only be configured by the browser platform administrator and cannot be over-ridden by the user when set according to policy. The TSS of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found the following functions are managed by an administrator and cannot be overridden: • Enabling and disabling storage of cookies (Cookies: Never) • Enabling and disabling the ability for websites to collect tracking information using cookies (Cookies: Never, From websites I visit, or From current website only) • Configuring the use of an application reputation service to detect malicious applications prior to download (Force fraud warning) • Configuring the use of a URL reputation service to detect sites that contain malware or phishing content (Force fraud warning) • Enabling and disabling JavaScript (JavaScript) Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.3.2 FMT_MOF_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to verify that it includes instructions for a browser platform administrator to configure the functions listed in FMT_MOF.1.1.
Evaluator Findings	The evaluator examined the operational guidance to verify that it includes instructions for a browser platform administrator to configure the functions listed in FMT_MOF.1.1. Section 5.4, “Cookie Blocking, Tracking Behavior, and Other Security Features,” within AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found the following administrative activities described: • To enable/disable storage of all cookies (including First-party cookies and Third party cookies), tap on Settings > Safari > Block All Cookies. • To clear your browser history and cookies, tap Settings > Safari > Clear History and Website Data. Clearing your history, cookies, and browsing data from Safari won't delete your AutoFill information. • To clear your AutoFill information, tap Settings > Safari > AutoFill. From here, you can toggle the information you wish to be saved, as well as review and delete saved information. • To clear your cookies and keep your history, tap Settings > Safari > Advanced > Website Data > Remove All Website Data. • To configure malicious application/URL detection, tap Settings > Safari > Fraudulent Website Warning. • To enable/disable JavaScript, tap Settings > Safari > Advanced > JavaScript. The evaluator found this to be consistent with the management activities described in the ST. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.4 FMT_SMF.1

5.4.4.1 FMT_SMF.1.1 Guidance

Objective	The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Evaluator Findings	The evaluator examined FMT_SMF.1 in the TSS in section 6 of the ST to determine what management functions are mandated by the PP. According to FMT_SMF.1 there are no management functions that the TSF must be able to perform. Because of this, there are no functions that must be described in the guidance and the assurance activity is considered satisfied. The evaluator verified that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function. Upon investigation, the evaluator found the following administrative activities described (Section 5.4, “Cookie Blocking, Tracking Behavior, and Other Security Features,” in AGD):

	- To enable/disable storage of all cookies (including First-party cookies and Third party cookies), tap on Settings > Safari > Block All Cookies. - To clear your browser history and cookies, tap Settings > Safari > Clear History and Website Data. Clearing your history, cookies, and browsing data from Safari won't delete your AutoFill information. - To clear your AutoFill information, tap Settings > Safari > AutoFill. From here, you can toggle the information you wish to be saved, as well as review and delete saved information. - To clear your cookies and keep your history, tap Settings > Safari > Advanced > Website Data > Remove All Website Data. - To configure malicious application/URL detection, tap Settings > Safari > Fraudulent Website Warning. - To enable/disable JavaScript, tap Settings > Safari > Advanced > JavaScript. The evaluator found these management activities to be all inclusive of the management activities required by the PP and EP. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Privacy)

5.5.1 FPR_ANO_EXT.1

5.5.1.1 FPR_ANO_EXT.1.1 TSS

Objective	The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.
Evaluator Findings	The evaluator examined the TSS section 6 “TOE Summary Specification” FPR_ANO_EXT.1 entry in Table 13 of the ST to identify functionality in the application where PII can be transmitted. Upon investigation, the evaluator found that the TOE does not specifically request PII from the user. Any information provided by the user is entered without prompting from the TOE. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Protection of the TSF)

5.6.1 FPT_API_EXT.1

5.6.1.1 FPT_API_EXT.1.1 TSS

Objective	The evaluator shall verify that the TSS lists the platform APIs used in the application.
Evaluator Findings	The evaluator examined the TSS section 6 “TOE Summary Specification” FPT_API_EXT.1 entry in Table 13 of the ST to determine if the platform APIs used in the application are listed. Upon investigation, the evaluator found that TSS lists the platform APIs used by the TOE. Based on this, the assurance activity is considered satisfied.

Verdict	Pass

5.6.2 FPT_AEX_EXT.1

5.6.2.1 FPT_AEX_EXT.1.1 TSS

Objective	The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.
Evaluator Findings	The evaluator examined the TSS section 6 “TOE Summary Specification” FPT_AEX_EXT.1 entry in Table 13 of the ST to determine if it describes the compiler flags used to enable ASLR. The TSS of the ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE is compiled with ASLR enabled. This is accomplished by being compiled with the -fPIE flag. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FPT_AON_EXT.1

5.6.3.1 FPT_AON_EXT.1.1 TSS

Objective	The evaluator shall verify that the TSS describes whether the browser is capable of loading trusted add-ons.
Evaluator Findings	The evaluator verified that the TSS describes whether the browser is capable of loading trusted add-ons. The TSS in section 6 “TOE Summary Specification” FPT_AON_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. The evaluator found that the TSS states that the TOE does not specifically request PII from the user. Any information provided by the user is entered without prompting from the TOE. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.3.2 FPT_AON_EXT.1.1 Guidance

Objective	The evaluator shall examine the operational guidance to verify that it includes instructions on loading trusted add-on sources.
Evaluator Findings	The evaluator shall examine the operational guidance to verify that it includes instructions on loading trusted add-on sources. Section 7, “Support for Add-ons,” of the AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE does not support add-ons. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.4 FPT_DNL_EXT.1

5.6.4.1 FPT_DNL_EXT.1.2 TSS

Objective	The evaluator shall examine the TSS to ensure that it describes the behavior of the browser when a user initiates the download of a file.
Evaluator Findings	The evaluator shall examine the TSS to ensure it lists the types of signed mobile

	code that the browser supports and describe how the browser handles unsigned mobile code, mobile code from an untrusted source, and mobile code from an unverified source. The TSS in section 6 “TOE Summary Specification” FPT_DNL_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the user must approve a request before the download begins or discard the download request. Only after the request is approved will the content be downloaded. The browser will not otherwise download the content. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.4.2 FPT_DNL_EXT.1.2 Guidance

Objective	The evaluator shall examine the operational guidance to ensure it describes the dialog box that appears when a download is initiated and the implications of the options presented by the dialog box.
Evaluator Findings	The evaluator shall examine the operational guidance to ensure it describes the dialog box that appears when a download is initiated and the implications of the options presented by the dialog box. Section 6.1, “File Downloads,” of the AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that AGD describes the dialog that is presented whenever any file is downloaded by the TOE. AGD also describes that without user interaction, the TOE will not download any file. Finally, an example of the dialog is presented. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.5 FPT_MCD_EXT.1

5.6.5.1 FPT_MCD_EXT.1.2 TSS

Objective	The evaluator shall examine the TSS to ensure it lists the types of signed mobile code that the browser supports. The TSS shall describe how the browser handles unsigned mobile code, mobile code from an untrusted source, and mobile code from an unverified source.
Evaluator Findings	The evaluator examined the TSS in section 6 “TOE Summary Specification” FPT_MCD_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. The evaluator found that the TOE does not support any types of mobile code. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.5.2 FPT_MCD_EXT.1.2 Guidance (TD0349)

Objective	If "provide the user with the option to discard" is selected, the evaluator shall examine the operational guidance to verify it provides configuration instructions for each of the supported mobile code types. The operational guidance shall also describes the alert that the browser displays to the user when unsigned, untrusted, or unverified mobile code is encountered and the actions the user can take.

	TD0349 has been applied.
Evaluator Findings	The TOE does not support any types of mobile code. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.6 FPT_TUD_EXT.1

5.6.6.1 FPT_TUD_EXT.1.1 Guidance

Objective	The evaluator shall check to ensure the guidance includes a description of how updates are performed.
Evaluator Findings	The evaluator checked section 2.2 “Installing Updates” of the AGD which describes how updates are performed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 FPT_TUD_EXT.1.2 Guidance

Objective	The evaluator shall verify guidance includes a description of how to query the current version of the application.
Evaluator Findings	The evaluator verified section 2.1 “Checking the Version” of the AGD describes detailed instructions on how to query the current version of the application. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.3 FPT_TUD_EXT.1.4 TSS (TD0561)

Objective	The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.
Evaluator Findings	The evaluator examined the TSS to determine if it identifies how the application installation package and updates to it are signed by an authorized source. Section 6 of the ST and the guidance document were used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE is provided within the underlying OS image and packaged as a signed IPA file. The platform considers the signature authorized if the certificate used to sign the IPA file chains to the Apple Worldwide Developer Relations Certification Authority or the Apple iPhone Certification Authority. Updates to the TOE are provided through underlying OS updates, and the current version of the TOE can be checked through the Settings app of the underlying platform. The ST (TSS) and the AGD are adequately consistent to ensure that they both describe how candidate updates are obtained. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.6.4 FPT_TUD_EXT.1.5 TSS

Objective	The evaluator shall verify that the TSS identifies how the application is distributed.
Evaluator Findings	The evaluator examined the TSS section 6 “TOE Summary Specification”

	FPT_TUD_EXT.1 entry in Table 13 to determine how the application is distributed. Upon investigation, the evaluator found that, "the TOE is provided within the underlying OS image and packaged as a signed IPA file." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.7 FPT_IDV_EXT.1

5.6.7.1 FPT_IDV_EXT.1 TSS

Objective	If "other version information" is selected the evaluator shall verify that the TSS contains an explaination of the versioning methodology.
Evaluator Findings	The evaluator checked the TSS in section 6 "TOE Summary Specification" FPT_IDV_EXT.1 entry in Table 13 of the ST which contains an explanation of the versioning methodology and was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states: "Each iOS and iPadOS application must be distributed as an Application Bundle. The Application Bundle includes an Info.plist file containing the following identifying information: Bundle name, Bundle ID, and Platform version (since the TOE is included with the platform OS). For the TOE, these are the following key/value pairs in the Info.plist file: • Bundle name: Safari • Bundle identifier: com.apple.mobilesafari • DTPlatformVersion: 14.6" Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.7 *TSS and Guidance Activities (Trusted Path)*

5.7.1 FTP_DIT_EXT.1

5.7.1.1 FTP_DIT_EXT.1 TSS [TD0444]

Objective	For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.
Evaluator Findings	The evaluator verified the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality. The TSS in section 6 "TOE Summary Specification" FTP_DIT_EXT.1 entry of Table 13 of the ST was used to determine the verdict of this activity. The evaluator found that the TOE invokes the platform provided HTTPS/TLS using the NSURLSession class. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Test Activities (Cryptographic Support)

6.1.1 FCS_RBG_EXT.1.1 Test 1 (TD0416, TD0510)

Item	Data/Description
Objective	If **invoke platform-provided DRBG functionality** is selected, the following tests shall be performed: The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API. The following are the per-platform list of acceptable APIs: **For iOS**: The evaluator shall verify that the application invokes either SecRandomCopyBytes, CCRandomGenerateBytes or CCRandomCopyBytes, or uses /dev/random directly to acquire random.
Test Flow	• View Safari source code. • In the source code, Search for “CCRandomGenerateBytes” • Verify that Safari invokes “CCRandomGenerateBytes”.
Expected Results	The TOE invokes CCRandomGenerateBytes.
Pass/Fail Explanation	Safari invokes CCRandomGenerateBytes. This meets the testing requirement.
Result	Pass

6.1.2 FCS_STO_EXT.1.1 Test 1

Item	Data/Description
Objective	For all credentials for which the application implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1(1) or conditioned according to FCS_CKM.1.1(1) and FCS_CKM.1(3). For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform. **For iOS**: The evaluator shall verify that all credentials are stored within a Keychain.
Test Flow	• Open the Settings app • Tap on Passwords and Accounts • Tap on Website & App Passwords • Verify that no credentials are stored in the Keychain • Start Safari • Navigate to https://mail.google.com • Tap Sign in

	• Enter a valid username • Tap Next • Enter a valid Password • Tap on Next • Safari will provide an opportunity to the user to Save these credentials to the Keychain • Tap on Save Password • Open the Settings app • Tap on Passwords and Accounts • Tap on Website & App Passwords • Verify that the credentials are now stored in the Keychain
Expected Results	The TOE stores credentials in the Keychain.
Pass/Fail Explanation	The TOE stores credentials in the Keychain.
Result	Pass

6.2 Test Activities (User Data Protection)

6.2.1 FDP_ACF_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall obtain or create JavaScript-based scripts that store and retrieve information from local and session storage and shall set up a web server with two or more web pages from different domains using different protocols and/or ports. The evaluator shall incorporate the scripts into the web pages and shall perform the following tests: The evaluator shall open two or more browser windows/tabs and navigate to the same page. The evaluator shall verify that the script for accessing session storage that is running on one window/tab cannot access session storage associated with a different window/tab.
Test Flow	• Start Safari ○ Establish a connection from Safari (Window 1/Tab 1) to Web Server 1. ○ Click on Set Session Storage ○ A Token value of "123456789" will be set. This is the default value provided by the website. ○ Establish another connection to the above website but this time in a different Window 2/Tab 2. ○ Verify that the token value from Window 1/ Tab 1 is not reflected in Window 2 / Tab 2. • Exit Safari.
Expected Results	Session storage value from Window 1 cannot be accessed by Window 2.
Pass/Fail Explanation	The evaluator observed that session storage on one window tab was not able to access session storage associated with a different tab. This meets the testing requirement.
Result	Pass

6.2.2 FDP_ACF_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall obtain or create JavaScript-based scripts that store and retrieve information from local and session storage and shall set up a web server with two or more web pages from different domains using different protocols and/or ports. The evaluator shall incorporate the scripts into the web pages and shall perform the following tests: The evaluator shall open windows/tabs and navigate to different web pages. The evaluator shall verify that a script running in the context of one domain/protocol/port in a browser window/tab cannot access information associated with a different domain/protocol/port in a different window/tab.
Pass/Fail Explanation	This test is performed in conjunction with FDP_SOP_EXT.1.2 Test #1. The TOE implements Same Origin Policy (SOP).
Result	Pass

6.2.3 FDP_COO_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall perform the following tests which may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products: The evaluator shall clear all cookies and then configure the browser so that storage of third party cookies is allowed. The evaluator shall load a web page that stores a third party cookie. The evaluator shall navigate to the location where cookies are stored and shall verify that the cookie is present.
Test Flow	• Steps to follow on the TOE/TOE platform: ○ Open the Settings app ○ Navigate to “Safari” ○ Verify Third Party Cookie storage is enabled. (Disable Block All Cookies) ○ Tap “Clear History and Data”. Tap “Clear” ○ Navigate to “Advanced” and Enable “Web Inspector” ○ Connect the TOE platform to the MacBook with a USB cable ○ Open Safari ○ Open https://www.tomshardware.com (Primary website/domain) • Steps to follow on the MacBook: ○ Start “Safari”. Click on “Preferences” and navigate to “Advanced” ○ Enable “Show Develop menu in menu bar” ○ Click on the “Develop” menu from menu bar. ○ Click on the connected TOE platform. Then click on the corresponding Safari instance. ○ Click on “Storage” and then click on “Cookies”. ○ Verify third party cookies are set on the TOE. (Cookies set by Third party domain pubmatic.com)
Expected Results	The evaluator should be able to view stored third party cookies.

Pass/Fail Explanation	The evaluator loaded a web page and verified that the third party cookie was stored.
Result	Pass

6.2.4 FDP_COO_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall perform the following tests which may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products: The evaluator shall clear all cookies and then configure the browser so that storage of third party cookies is blocked (i.e. not allowed). The evaluator shall load a web page that attempts to store a third party cookie and shall verify that the cookie was not stored.
Test Flow	• Steps to follow on iOS Device (iPhone/iPad): ○ Within iPad navigate to “Settings” ○ Navigate from “Settings” to “Safari” ○ Verify Third Party Cookie storage is disabled. (Enable Block All Cookies) ○ Within “Safari” navigate to “Advanced” and Enable “Web Inspector” ○ Open https://www.tomshardware.com (Primary website/domain) • Steps to follow on Macbook: ○ Start “Safari” on Macbook. Click on “Preferences” and Navigate to “Advanced”. ○ Enable “Show Develop menu in menu bar” and Exit. ○ Within “Safari”, click on “Develop” menu from menu bar. ○ Click on the connected iOS device. Then click on the corresponding Safari instance. ○ Click on “Storage” and then click on “Cookies”. ○ Verify third party cookies are not set on the TOE.
Expected Results	Safari does not store any cookies after “Block All Cookies” option is enabled.
Pass/Fail Explanation	The evaluator loaded a web page and verified that the cookie was not stored.
Result	Pass

6.2.5 FDP_DEC_EXT.1.1 Test 1

Item	Data/Description
Objective	**For iOS**: The evaluator shall verify that either the application or the documentation provides a list of the hardware resources it accesses.
Test Flow	• Verify TOE documentation provides a list of required hardware resources.
Expected Results	The TOE documentation provides a list of required hardware resources.
Pass/Fail Explanation	This is satisfied by the FDP_DEC_EXT.1.1 Guidance Evaluation Activity.
Result	Pass

6.2.6 FDP_DEC_EXT.1.2 Test 1

Item	Data/Description
Objective	**For iOS**: The evaluator shall verify that either the application software or its documentation provides a list of the sensitive information repositories it accesses.
Test Flow	• Verify TOE documentation provides a list of required sensitive information repositories.
Expected Results	The TOE documentation provides a list of required sensitive information repositories the TOE accesses.
Pass/Fail Explanation	This is satisfied by the FDP_DEC_EXT.1.2 Guidance Evaluation Activity.
Result	Pass

6.2.7 FDP_NET_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.
Note	This test is performed in conjunction with FTP_DIT_EXT.1 Test #2
Expected Results	The TOE only performs user-initiated network communications.
Pass/Fail Explanation	The TOE only sends user-initiated TLS traffic as expected.
Result	Pass

6.2.8 FDP_NET_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).
Test Flow	• TCP • Perform a TCP port scan prior to exercising the application • Initialize and engage with the application to perform some activity. • Perform a TCP port scan after exercising the application • UDP • Perform a UDP port scan prior to exercising the application • Initialize and engage with the application to perform some activity. • Perform a UDP port scan after exercising the application
Expected Results	The TOE does not open any new ports.
Pass/Fail Explanation	The TOE did not open any ports.
Result	Pass

6.2.9 FDP_DAR_EXT.1.1 Test 1

Item	Data/Description

Objective	*Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.* *The evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.*
Test Flow	• Determine where the TOE may write data and ensure the data is stored encrypted.
Expected Results	The TOE stores data in the application working directory with an appropriate data protection class (that ensures the data is encrypted).
Pass/Fail Explanation	This is satisfied by the FPT_AEX_EXT.1.4 Test 1 and FDP _DAR_EXT.1.1 Test 2. iOS forces applications to write all data within the application working directory. The TOE stores data using Class A protection.
Result	Pass

6.2.10 FDP_DAR_EXT.1.1 Test 2

Item	Data/Description
Objective	*Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.* *If* ***leverage platform-provided functionality*** *is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis:* ***For iOS****: The evaluator shall inspect the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally.*
Test Flow	• Examine the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally.
Expected Results	The TSS Describes the data protection class(es) the TOE uses to store files.
Pass/Fail Explanation	This is satisfied by the FDP_DAR_EXT.1.1 TSS Evaluation Activity.
Result	Pass

6.2.11 FDP_SBX_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall execute a form of mobile code within an HTML page that contains instructions to modify or delete a file from the file system and verify that the file is not modified for deleted.
Test Flow	• Browse to https://www.adobe.com/shockwave/welcome/index.html
Expected Results	The TOE does not execute the shockwave player (it is rendered by Shockwave).
Pass/Fail Explanation	The TOE does not execute mobile code, so mobile code cannot modify or delete a file from the filesystem.
Result	Pass

6.2.12 FDP_SOP_EXT.1.2 Test 1

Item	Data/Description
Objective	The evaluator shall obtain or create scripts that can retrieve content from designated locations and shall set up a web server with two or more web pages representing different domains. The evaluator shall incorporate the scripts into the web pages. The evaluator shall associate each page with a different protocol and/or port and shall perform the following tests: The evaluator shall open two or more browser windows/tabs and navigate to a different page on the website in each window/tab. The evaluator shall run the scripts and shall verify that the script that is running in one window/tab cannot access content that was retrieved in a different window/tab.
Test Flow	• Go to the Settings app • Scroll down and tap on Safari • Scroll down and tap on "Clear History and Website Data" • Start Safari. Open a new tab • Navigate to Web Server 1 port 4444. This will set the Cookie value to "testcookie" • Open a new tab on TOE and navigate to Web Server 2 port 4445 • Verify that Web Server 2 port 4445 is not able to access the Cookie value "testcookie". i.e., "Cookie is null" is displayed on TOE
Expected Results	Script running in one window cannot access content that was retrieved in a different window.
Pass/Fail Explanation	Script running in one tab cannot access content that was retrieved in a different tab.
Result	Pass

6.2.13 FDP_SOP_EXT.1.2 Test 2

Item	Data/Description
Objective	The evaluator shall obtain or create scripts that can retrieve content from designated locations and shall set up a web server with two or more web pages representing different domains. The evaluator shall incorporate the scripts into the web pages. The evaluator shall associate each page with a different protocol and/or port and shall perform the following tests: The evaluator shall verify that the scripts can retrieve content from another window/tab at a different subdomain.
Test Flow	• Start Safari and navigate to http://sub1.acumensec.local • Record the cookie set by sub1.acumensec.local. Note: the cookie is set with domain=acumensec.local • Open a new tab and navigate to http://sub2.acumensec.local • Verify the script running in the second tab can retrieve the cookie set by sub1.acumensec.local
Expected Results	The TOE allows the script to retrieve content from another tab at a different subdomain.
Pass/Fail Explanation	The script running in the second tab can retrieve the cookie set by a different subdomain.
Result	Pass

6.2.14 FDP_STR_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall perform the following tests which may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products: The evaluator shall connect the browser to a cookie-enabled test website implementing HTTPS and have the website present the browser with a "secure" cookie. The evaluator shall examine the browser's cookie cache and verify that that it contains the secure cookie.
Test Flow	• Connect to a HTTPS website that presents a cookie with the secure flag • Verify the cookie is stored in the TOE's cookie cache, and verify the secure flag is included • Connect to the same website over HTTP and verify the secure cookie is not sent to the website
Expected Results	The TOE stores "secure" cookies in its cache with the secure flag.
Pass/Fail Explanation	When the TOE connected to a cookie-enabled test website implementing HTTPS the evaluator examined the browser's cookie cache and verified that it contained the secure cookie with the secure flag.
Result	Pass

6.2.15 FDP_STR_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall perform the following tests which may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products: The evaluator shall reconnect to the cookie-enabled website over an insecure channel and verify that no "secure" cookie is sent.
Expected Results	The TOE does not send "secure" cookies over HTTP.
Pass/Fail Explanation	This test is performed as part of FDP_STR_EXT.1.1 Test 1. The TOE did not send the secure cookie to the website over an insecure channel.
Result	Pass

6.2.16 FDP_TRK_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall perform the following tests for each type of tracking information listed in the TSS: The evaluator shall configure a website that requests the tracking information about the user and shall navigate to that website. The evaluator shall verify that the user is notified about the request for tracking information and that, upon consent, the web browser retrieves the tracking information.
Test Flow	• Go to a website that requests location tracking information • Verify the user is prompted to approve sharing the tracking information • Provide consent for sharing the tracking information • Verify the tracking information is shared with the website
Expected Results	Safari presents the user with the request for sharing location tracking information with a website and, upon consent, sends the tracking information to the website.

Pass/Fail Explanation	Safari notifies the user about location tracking requests and, upon consent, shares the tracking information.
Result	Pass

6.2.17 FDP_TRK_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall perform the following tests for each type of tracking information listed in the TSS: The evaluator shall verify that the user is notified about the request for tracking information and that, when rejected, the browser does not provide the tracking information.
Test Flow	• Go to a website that requests location tracking information • Verify the user is prompted to approve sharing the tracking information • Withhold consent for sharing the tracking information • Verify the tracking information is not shared with the website
Expected Results	Safari presents the user with the request for sharing location tracking information with a website and, when denied, does not send the tracking information to the website.
Pass/Fail Explanation	Safari notifies the user about location tracking requests and, upon denial, does send tracking information to the website.
Result	Pass

6.3 Test Activities (Identifiation and Authentication)

6.3.1 FIA_X509_EXT.1.1 Test 1 (TD0587)

Item	Data/Description
Objective	Test 1: The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: • by establishing a certificate path in which one of the issuing certificates is not a CA certificate, • by omitting the basicConstraints field in one of the issuing certificates, • by setting the basicConstraints field in an issuing certificate to have CA=False, • by omitting the CA signing bit of the key usage field in an issuing certificate, and • by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails.
Test Steps	• Establish a connection to a remote server following each step in the assurance activity. • Show the TOE rejects invalid certificate configurations • Show the TOE accepts a complete valid certificate chain

Expected results	The TOE rejects the connection and prompts the user to either trust the certificate, check the details of the certificate or keep rejecting the certificate. Only the end entity certificate details can be displayed on the TOE. The packet captures will show the certificate chain details.
Pass/Fail Explanation	The TOE accepts or rejects a connection to remote entity depending on the certificate chain validity.
Result	Pass

6.3.2 FIA_X509_EXT.1.1 Test 2 (TD0587)

Item	Data/Description
Objective	Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• Attempt a connection to a server using an expired certificate • Show the TOE rejects the certificate
Expected Results	The TOE rejects the expired certificate.
Pass/Fail Explanation	The TOE rejected a connection to a remote entity using an expired certificate.
Result	Pass

6.3.3 FIA_X509_EXT.1.1 Test 3 (TD0587)

Item	Data/Description
Objective	Test 3: The evaluator shall test that the TOE can properly handle revoked certificates-"conditional on whether CRL, OCSP, OCSP Stapling or OCSP Multi-stapling is selected; if multiple methods are selected, then the following tests shall be performed for each method: The evaluator shall test revocation of the node certificate. The evaluator shall also test revocation of an intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA), if intermediate CA certificates are supported. If OCSP stapling per RFC 6066 is the only supported revocation method, this test is omitted. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.
Test Steps	• initiate a connection to a remote TLS server using a valid certificate • show the certificate is accepted and the connection succeeds • initiate a new connection to the same server using a revoked certificate • show the certificate is rejected and the connection is denied
Expected Results	The TOE validates a certificate after receiving a valid and "good" OCSP response and sends application data. The TOE rejects the remote server certificate after receiving a valid and "revoked" OCSP response and terminates the connection.
Pass/Fail with Explanation	The TOE accepts good certificates and rejects revoked certificates.
Result	Pass

6.3.4 FIA_X509_EXT.1.1 Test 4 (TD0587)

Item	Data/Description
Objective	Test 4: If any OCSP option is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set, and verify that validation of the CRL fails.
Test Steps	• attempt a connection to a server using an OCSP signing certificate missing the OCSP Signing ExtendedKeyUsage while sending a revoked status • show the validation of the response fails and the TOE accepts the connection
Expected Results	The TOE rejects the OCSP response and connects successfully to the remote server.
Pass/Fail Explanation	The invalid OCSP response is rejected and the TOE accepts the connection.
Result	Pass

6.3.5 FIA_X509_EXT.1.1 Test 5 (TD0587)

Item	Data/Description
Objective	Test 5: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• Attempt a connection to a remote TLS server running Acumen-TLS tool that would perform the modification on the certificate’s first eight bytes • Show the TOE rejects the certificate, and the TLS handshake does not successfully complete
Expected Results	The TOE rejects the connection due to the server certificate being invalid.
Pass/Fail Explanation	The TOE rejects a leaf certificate that has had modification done in the first eight bytes.
Result	Pass

6.3.6 FIA_X509_EXT.1.1 Test 6 (TD0587)

Item	Data/Description
Objective	Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Attempt a connection to a remote TLS server running Acumen-TLS tool that would perform the modification on the certificate last byte • Show the TOE rejects the certificate, and the TLS handshake does not successfully complete
Expected results	The TOE rejects the connection due to the server certificate being invalid.
Pass/Fail Explanation	The TOE rejects a leaf certificate that has a modified signature.
Result	Pass

6.3.7 FIA_X509_EXT.1.1 Test 7 (TD0587)

Item	Data/Description
Objective	Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Attempt a connection to a remote TLS server running Acumen-TLS tool that would perform the modification on the certificate public key • Show the TOE rejects the certificate, and the TLS handshake does not successfully complete
Expected results	The TOE rejects the connection due to the server certificate being invalid
Pass/Fail Explanation	Pass. The TOE rejects a leaf certificate that has had modifications done to the public key.
Result	Pass

6.3.8 FIA_X509_EXT.1.2 Test 1 (TD0495)

Item	Data/Description
Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. The evaluator shall ensure that the certificate of at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator shall confirm that validation of the certificate path fails: (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate without the basicConstraints extension to the TOE's trust store.
Test Steps	N/A
Pass/Fail Explanation	The test is satisfied by FIA_X509_EXT.1.1 Test 1.
Result	Pass

6.3.9 FIA_X509_EXT.1.2 Test 2 (TD0495)

Item	Data/Description
Objective	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules.

	If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. The evaluator shall ensure that the certificate of at least one of the CAs in the chain has the CA flag in the basicConstraints extension not set (or set to FALSE). The evaluator shall confirm that validation of the certificate path fails (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate with the CA flag not set (or set to FALSE) in the basicConstraints extension to the TOE's trust store
Test Steps	N/A
Pass/Fail Explanation	The test is satisfied by FIA_X509_EXT.1.1 Test 1.
Result	Pass

6.3.10 FIA_X509_EXT.2.2 Test 1

Item	Data/Description
Objective	The evaluator shall perform the following test for each trusted channel: Test 1: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps	• Attempt a connection to a remote TLS server using a valid certificate and an invalid OCSP status response • Show the TOE accepts the certificate
Expected Results	The TOE accepts the certificate when the certificate validation cannot be determined.
Pass/Fail Explanation	The TOE accepts the remote entity’s certificate if the certificate validation fails.
Result	Pass

6.3.11 FIA_X509_EXT.2.2 Test 2

Item	Data/Description
Objective	The evaluator shall perform the following test for each trusted channel:

	Test 2: The evaluator shall demonstrate that an invalid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity cannot be accepted.
Test Steps	• Attempt a connection to a remote TLS server using an invalid certificate and an invalid OCSP response • Show the TOE rejects the connection
Expected Results	The TOE rejects a certificate that is invalid and receives an invalid OCSP stapling response.
Pass/Fail Explanation	The TOE rejects an invalid certificate that requires certificate validation.
Result	Pass

6.4 Test Activities (Security Management)

6.4.1 FMT_MEC_EXT.1.1 Test 1 (TD0437)

Item	Data/Description
Objective	If “invoke the mechanisms recommended by the platform vendor for storing and setting configuration options” is chosen, the method of testing varies per platform as follows: **For iOS**: The evaluator shall verify that the app uses the user defaults system or key-value store for storing all settings.
Test Flow	• ssh into the device • Execute command: defaults read | grep safari • Execute command: defaults read com.apple.SafariBookmarksSyncAgent.XPC.CloudTabsZoneSubscriptionRegistration • Execute command: defaults read com.apple.SafariBookmarksSyncAgent.XPC.PeriodicRemoteMigrationStateObserver • Execute command: defaults read com.apple.SafariBookmarksSyncAgent.XPC.ZoneSubscriptionRegistration • Execute command: defaults read com.apple.SafariBookmarksSyncAgent.migration
Expected Results	The TOE uses the user defaults system to store all settings.
Pass/Fail Explanation	The TOE uses the user defaults system for storing all settings.
Result	Pass

6.4.2 FMT_CFG_EXT.1.1 Test 1

Item	Data/Description
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality

	required to set new credentials is available.
Pass/Fail Explanation	The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.
Result	Pass

6.4.3 FMT_CFG_EXT.1.1 Test 2

Item	Data/Description
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail Explanation	The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.
Result	Pass

6.4.4 FMT_CFG_EXT.1.1 Test 3

Item	Data/Description
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.
Pass/Fail Explanation	The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.
Result	Pass

6.4.5 FMT_CFG_EXT.1.2 Test 1

Item	Data/Description
Objective	The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform. **For iOS**: The evaluator shall determine whether the application leverages the appropriate Data Protection Class for each data file stored locally.
Test Flow	• Verify Apple developer specific access is granted to the TOE. • Start the device, but do not unlock the device. • Dump the device memory. • Verify Class A (keyID 1) keys are not present in the memory dump. • Unlock the device for the first time. • Dump the device memory and observe that a Class A key is present. • Lock the device. Dump the device memory again. • Verify Class A (keyID 1) keys are not present in the memory dump. • Unlock the device a second time. • Dump the device memory and observe that Class A key is present.
Expected Results	Safari stores its files using the Class A data protection class.
Pass/Fail Explanation	The TOE uses Data Protection Class A – Complete Protection. This meets the testing requirement.

Result	Pass

6.4.6 FMT_MOF_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall verify that functions perform as intended by enabling, disabling, and configuring the functions.
Test Flow	• Attempt to perform the management functions claimed in FMT_MOF_EXT.1.1. • Verify the functions can be configured.
Expected Results	The TOE is capable of performing the management functions claimed in the ST.
Pass/Fail Explanation	The tester verified that Safari management functions can be enabled, disabled and configured as intended.
Result	Pass

6.4.7 FMT_MOF_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall create policies that collectively include all management functions controlled by the browser platform administrator and cannot be over-ridden by the user as defined in FMT_MOF.1.1. The evaluator shall apply these policies to the browser, attempt to override each setting as the user, and verify that the browser does not permit it.
Expected Results	The administrator is able to enforce management functions that the user cannot override.
Pass/Fail with Explanation	Pass. The TOE allows an administrator to set policies using a profile and won't allow a user to override them.
Result	Pass

6.4.8 FMT_SMF.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Pass/Fail Explanation	This test was performed in conjunction with FMT_MOF_EXT.1.1 Test 1. Configuration of the TOE is available as expected.
Result	Pass

6.5 Test Activities (Privacy)

6.5.1 FPR_ANO_EXT.1.1 Test 1

Item	Data/Description
Objective	If require user approval before executing is selected, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII.
Pass/Fail Explanation	This test is not applicable, because the ST does not select 'require user approval before executing'.
Result	Pass

6.6 Test Activities (Protection of the TSF)

6.6.1 FPT_API_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.
Test Flow	• Search the platform developer references for each API listed in the TSS. • Verify all APIs are supported.
Expected Results	All APIs used by the TOE are supported.
Pass/Fail Explanation	All APIs used by the TOE are supported.
Result	Pass

6.6.2 FPT_AEX_EXT.1.1 Test 1 (TD0544)

Item	Data/Description
Objective	The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings. **For iOS**: The evaluator shall perform a static analysis to search for any mmap calls (or API calls that call mmap), and ensure that no arguments are provided that request a mapping at a fixed address.
Test Flow	• Navigate to Safari source directory • Execute grep -r mmap *
Expected Results	The TOE does not make any calls to mmap in a way that would result in memory being mapped to a fixed address.
Pass/Fail Explanation	The TOE does not make any calls to mmap.
Result	Pass

6.6.3 FPT_AEX_EXT.1.2 Test 1

Item	Data/Description
Objective	The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform. **For iOS**: The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission.
Test Flow	• Navigate to Safari source directory • Execute grep -r PROT_EXEC * • Verify that mprotect is never invoked with PROT_EXEC permission
Expected Results	The TOE does not invoke mprotect with the PROT_EXEC permissions.
Pass/Fail Explanation	The TOE does not invoke mprotect with the PROT_EXEC permission. This meets the testing requirement.

Result	Pass

6.6.4 FPT_AEX_EXT.1.3 Test 1

Item	Data/Description
Objective	The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests: **For iOS**: Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required.
Pass/Fail Explanation	Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required.
Result	Pass

6.6.5 FPT_AEX_EXT.1.4 Test 1

Item	Data/Description
Objective	The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform: **For iOS**: The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).
Pass/Fail Explanation	This requirement is implicitly met based on the Assurance Activity.
Result	Pass

6.6.6 FPT_AEX_EXT.1.5 Test 1

Item	Data/Description
Objective	The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present. Tools such as Canary Detector may help automate these activities.
Test Flow	• Verify the presence of the ___stack_chk_fail and/or ___stack_chk_guard symbols in the compiled TOE application.
Expected Results	The TOE is compiled with stack-based buffer overflow protections.
Pass/Fail Explanation	The TOE contains the ___stack_chk_fail and ___stack_chk_guard symbols, indicating that the TOE was compiled with stack smashing protections.
Result	Pass

6.6.7 FPT_AON_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall create or obtain an untrusted add-on and attempt to load it. The evaluator shall verify that the untrusted add-on is rejected and cannot be loaded.
Pass/Fail Explanation	The TOE does not support add-ons. Therefore, this requirement is met implicitly.
Result	Pass

6.6.8 FPT_AON_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall create or obtain a trusted add-on and attempt to load it. The evaluator shall verify that the trusted add-on loads.
Pass/Fail Explanation	The TOE does not support add-ons. Therefore, this requirement is met implicitly.
Result	Pass

6.6.9 FPT_DNL_EXT.1.2 Test 1

Item	Data/Description
Objective	The evaluator shall navigate to a website that hosts files for download including executables and shall attempt to download and open several of these files. The evaluator shall verify that the browser always presents a dialog box with the option to either download the file to the file system or to discard the file.
Test Flow	• Start Safari Browser. • Connect to Web Server 1 port 7776 in Safari. ○ Click on “Download Sample Executable” (MS Windows Application) ▪ A dialog box is presented to the user that gives the user an opportunity to Download or Discard (X symbol) the file. ▪ Click on “Download”. Verify the file is Downloaded (this can be verified by observing the Download Arrow in Blue color next to the Address Bar) ▪ Click on the Download Arrow. This will show the Downloaded file(s). ▪ Attempt to open the Downloaded file. ○ Click on “Download Sample Security Certificate” ▪ A dialog box is presented to the user that gives the user an opportunity to Download (Allow) or Discard (Ignore) the file. ▪ Click on “Allow”. iOS/iPadOS will show a Notification to the User “Profile Downloaded: Review the profile in Settings app if you want to install it”. ○ Click on “Download Sample DEB File” (Debian Package) ▪ A dialog box is presented to the user that gives the user an opportunity to Download or Discard (X symbol) the file. ▪ Click on “Download”. Verify the file is Downloaded (this can be verified by observing the Download Arrow in Blue color next to the Address Bar) ▪ Click on the Download Arrow. This will show the Downloaded file(s). ▪ Attempt to open the Downloaded file. ○ Click on “Download Sample IPA File” (iOS Package) ▪ A dialog box is presented to the user that gives the user an opportunity to Download or Discard (X symbol) the

	file. ▪ Click on “Download”. Verify the file is Downloaded (this can be verified by observing the Download Arrow in Blue color next to the Address Bar) ▪ Click on the Download Arrow. This will show the Downloaded file(s). ▪ Attempt to open the Downloaded file. • Exit Safari Browser.
Expected Results	The browser presents a dialog box with the option to either download the file to the file system or to discard the file.
Pass/Fail Explanation	The TOE presents a dialog box with the option to either download the file to the file system or discard the file.
Result	Pass

6.6.10 FPT_MCD_EXT.1.2 Test 1 (TD0349)

Item	Data/Description
Objective	The evaluator shall perform the following test for each mobile code type specified in the TSS: The evaluator shall construct a web page containing correctly signed mobile code and show that it is accepted and executes. The evaluator shall then construct three web pages containing unacceptable mobile code: the first web page contains mobile code that is unsigned; the second web page contains mobile code that is untrusted; the third web page contains mobile code that is unverified. The evaluator shall then attempt to load the mobile code from each of the three web pages, and observe that either 1) the code is rejected, or 2) the user is prompted to accept or reject the code; when the user rejects the code, the code is not executed.
Pass/Fail Explanation	N/A – The TSS does not specify any types of mobile code.
Result	Pass

6.6.11 FPT_TUD_EXT.1.1 Test 1

Item	Data/Description
Objective	The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.
Test Flow	• Tap “Settings” • Tap “General” • Tap “About” • Verify the current version of the platform and TOE is displayed • Tap “< General” • Tap “Software Update” • Verify the platform reports whether an update is available
Expected Results	The platform displays the current version of the platform and TOE. The platform checks for updates and indicates if an update is available.

Pass/Fail Explanation	The TOE platform successfully checks for updates and indicates no update is available.
Result	Pass

6.6.12 FPT_TUD_EXT.1.2 Test 1

Item	Data/Description
Objective	The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.
Expected Results	The current version of the TOE can be queried and matches the documentation.
Pass/Fail Explanation	This test is performed in conjunction with FTP_TUD_EXT.1.1 Test 1. The TOE platform displays the current version of the TOE.
Result	Pass

6.6.13 FPT_TUD_EXT.1.3 Test 1 (TD0548)

Item	Data/Description
Objective	For iOS: The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).
Pass/Fail Explanation	The requirement is considered met because the platform forces applications to write all data within the application working directory (sandbox).
Result	Pass

6.6.14 FPT_TUD_EXT.1.5 Test 1

Item	Data/Description
Objective	If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS.
Test Flow	• Go to Settings > General > Reset > Erase All Content and Settings • Tap Erase Now • Enter the passcode • Tap Erase iPhone/iPad • Verify the TOE is present after the erase completes
Expected Results	The TOE is a default app that come with the platform.
Pass/Fail Explanation	The TOE is present after performing a factory reset.
Result	Pass

6.6.15 FPT_LIB_EXT.1 Test 1

Item	Data/Description
Objective	The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Test Flow	• ssh into the device • Execute command: cd /Applications/MobileSafari.app • Execute command: ls -alR

	- Verify that no third-party libraries are installed
Expected Results	The survey of the directories shows that there are no third-party libraries installed.
Pass/Fail Explanation	The TOE is installed with no third-party libraries. These meets the testing requirements.
Result	Pass

6.6.16 FPT_IDV_EXT.1 Test 1

Item	Data/Description
Objective	The evaluator shall install the application, then check for the / existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.
Test Flow	• Open and inspect Info.plist file • Verify the TOE is identified by the Platform Version, Display Name, and Bundle ID parameters.
Expected Results	The info.plist file shows the TOE is identified with a Platform Version, Display Name, and Bundle ID that match the ST.
Pass/Fail Explanation	The evaluator verified that the TOE was identified correctly.
Result	Pass

6.7 Test Activities (Trusted Path)

6.7.1 FTP_DIT_EXT.1.1 Test 1 (TD0444)

Item	Data/Description
Objective	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST.
Expected Results	The TOE sends all traffic via HTTLS/TLS.
Pass/Fail Explanation	All TOE communications are over HTTPS/TLS.
Result	Pass

6.7.2 FTP_DIT_EXT.1.1 Test 2

Item	Data/Description
Objective	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear.
Test Flow	• Initialize Safari. • Establish a connection to https://security.stackexchange.com • Enter User credentials and Login to the web application. • Verify no sensitive data is transmitted in the clear
Expected Results	All sensitive data are encrypted and not visible when capturing the traffic

	coming from the TOE.
Pass/Fail Explanation	The TOE does not send any sensitive data in plaintext.
Result	Pass

6.7.3 FTP_DIT_EXT.1.1 Test 3

Item	Data/Description
Objective	The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found.
Pass/Fail Explanation	The TOE does not transmit "TOE credentials." In FTP_DIT_EXT.1.1 Test 2, website credentials were used as the sensitive data. The plaintext website credentials were not found in the packet capture.
Result	Pass

6.7.4 FTP_DIT_EXT.1.1 Test 4

Item	Data/Description
Objective	**For iOS**: If "encrypt all transmitted data" is selected, the evaluator shall ensure that the application's Info.plist file does not contain the NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys, as these keys disable iOS's Application Transport Security feature.
Test Flow	• ssh into the device. • cd into Applications/MobileSafari.app • Open the info.plist file • Verify that the file does not contain NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys
Expected Results	The info.plist file does not contain the keys that disable iOS's Application Transport Security feature.
Pass/Fail Explanation	A search for both the keywords yielded no results.
Result	Pass

7 Security Assurance Requirements

7.1 ADV_FSP.1 TSS

Objective	There are no specific evaluation activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in 5.1 Security Functional Requirements, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.
Evaluator Findings	The evaluator found that all assurance activities were able to be performed and all interfaces were specified in a way that allowed this to occur. Based on these findings, this work unit is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Guidance

Objective	Some of the contents of the operational guidance will be verified by the evaluation activities in 5.1 Security Functional Requirements and evaluation of the TOE according to the [CEM]. The following additional information is also required. If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform. The evaluator shall verify that this process includes the following steps: • Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). • Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.
Evaluator Findings	Section 3 of the AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the TOE does not directly provide any cryptography. Instead the TOE leverages the platform cryptography. The evaluator also found that there is no configuration required to leverage the crypto. In addition, section 2 of the AGD was used to determine the verdict of this work

	unit. Upon investigation, the evaluator found that guidance describes that the application is updated as part of the overall product update. It is not updated separately. The steps for checking for an OS update are also described. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Guidance

Objective	As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.
Evaluator Findings	Section 1 of the AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes the platform on which the TOE resides. Table 1 of the AGD identifies each of the platforms. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC_CMC.1 TSS

Objective	The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.
Evaluator Findings	The evaluator examined the ST to ensure that it contains an identifier that specifically identifies the version that meets the requirement of the ST. Section 1.1 of the ST was used to determine the verdict of this assurance activity. The evaluator found that the TOE is identified as Apple iOS 14 and iPadOS 14: Safari. This is consistent with how the product is identified in the guidance document and on Apple Software's product website. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

7.5 ALC_CMS.1 TSS & Guidance

Objective	The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a

	developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation. The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.
Evaluator Findings	As stated in other assurance activities, the TOE has been uniquely identified and all identifying information is consistent. The TSS in section 6 "TOE Summary Specification" FPT_AEX_EXT.1 entry listed in Table 13 of the ST identifies how (stack-based) buffer overflow protection is enabled Based on this, the assurance activity is considered satisfied.
Verdict	Pass

7.6 ALC_TSU_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.
Evaluator Findings	The evaluator examined the ALC_TSU_EXT.1 entry in Table 13 of the ST and found that the entry contains a description of how security updates are created and deployed. Upon investigation, the evaluator found that updates are provided using the platform update mechanisms and delivered as part of a system update. If a security vulnerability is identified for the TOE, the vendor provides the Apple Support web page to report problems and the vendor will also provide an update.
Verdict	Pass

7.7 ALC_TSU_EXT.1 TSS 2

Objective	The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.

	The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.
Evaluator Findings	The evaluator verified that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The ALC_TSU_EXT.1 row of Table 13 of the ST says the vendor performs a full investigation and creates necessary patches. The evaluator verified that the description includes publicaly available mechanisms for reporting security issues related to the TOE. The ALC_TSU_EXT.1 row of Table 13 of the ST says security issues can be reported on the vendor website (secured using HTTPS) or through email (secured through PGP). Based on these findings, the assurance activity is considered satisfied.
Verdict	Pass

7.8 ATE_IND.1 Test 1

Objective	The evaluator shall prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP's evaluation activities. While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no effect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (e.g SSH). The

	test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.
Evaluator Findings	In support of the AAs in the PP, the evaluator created a test plan. This test plan includes an equivalency argument, a description of the test infrastructure (including the host platforms), each test case, and actual results for each test case. Based on these findings, this work unit is considered satisfied.
Verdict	Pass

7.9 AVA_VAN.1 Test 1

Objective	The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The public search for vulnerabilities was performed on July 14, 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:14.6:*:*:*:*:*:*:* • cpe:2.3:o:apple:iphone_os:14.6:*:*:*:*:*:*:*

	No publicly known vulnerabilities were discovered in the TOE.
Verdict	Pass

8 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date that are applicable to [SWAPP] and [WEBBROWSEREP] have been considered. The following tables identifies all applicable TD:

Table 5 – Techincal Decisions

Identifier	Applicable	Exclusion Rationale (if applicable)
TD0349: Update to FPT_MCD_EXT.1.2	Yes	
TD0416: Correction to FCS_RBG_EXT.1 Test Activity	Yes	
TD0427: Reliable Time Source	Yes	
TD0434: Windows Desktop Applications Test	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
TD0437: Supported Configuration Mechanism	Yes	
TD0445: User Modifiable File Definition	Yes	
TD0465: Configuration Storage for .NET Apps	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0473: Support for Client or Server TOEs in FCS_HTTPS_EXT	No	The TOE uses platform-provided HTTPS, so it does not include FCS_HTTPS_EXT.1.
TD0495: FIA_X509_EXT.1.2 Test Clarification	No	The TOE does not directly invoke X.509 functionality.
TD0498: Application Software PP Security Objectives and Requirements Rationale	Yes	
TD0510: Obtaining random bytes for iOS/macOS	Yes	
TD0515: Use Android APK manifest in test	No	This TD only applies to Android platforms. The TOE runs on iOS and iPadOS.
TD0519: Linux symbolic links and FMT_CFG_EXT.1	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
TD0540: Expanded AES Modes in FCS_COP	No	The TOE does not implement AES.
TD0543: FMT_MEC_EXT.1 evaluation activity update	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0544: Alternative testing methods for FPT_AEX_EXT.1.1	Yes	
TD0548: Integrity for installation test in AppSW PP 1.3	Yes	
TD0554: iOS/iPadOS/Android AppSW Virus Scan	Yes	
TD0561: Signature verification update	Yes	
TD0582: PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed	Yes	
TD0587: X.509 SFR Applicability in App PP	Yes	

9 Conclusions

All testing and assurance activities pass.

---End of Document---