Apple iOS and iPadOS 13 Safari Security Target

Prepared for Apple Inc.

Prepared by Acumen Security, LLC.

Document Version: 1.1

Table Of Contents

Revision History

Version	Date	Description
0.1	October 2019	Initial Draft
0.2	October 2019	Minor Updates
0.3	November 2019	Updated based on internal review
0.4	March 2020	Updated TDs
0.5	May 2020	Updated for submission.
1.0	June 2020	Updated based on ECR comments.
1.1	June 2020	Updated device identifiers

1 Security Target Introduction

1.1 Security Target and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Category	Identifier
ST Title	Apple iOS and iPadOS 13 Safari Security Target
ST Version	1.1
ST Date	June 2020
ST Author	Acumen Security, LLC.
TOE Identifier	Apple iOS and iPadOS 13: Safari
TOE Software Version	13.4.1
TOE Developer	Apple Inc.
Key Words	Application, Mobility, Browser

Table 1 TOE/ST Identification

1.2 TOE Overview

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

Note: The TOE is the Safari software only. The Apple iOS and iPadOS operating systems have been separately validated.

1.3 TOE Description

1.3.1 Evaluated Configuration

The TOE is an application on a mobile operating system. The TOE is the Safari browser application only. The Apple iOS and iPadOS operating systems have been separately validated against the Protection Profile for Mobile Device Fundamentals Version 3.1. The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 13.4.1.

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

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11 Pro	A2160 A2215 A2216 A2217	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11	A2111 A2221 A2222 A2223	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone SE (2nd Gen)	A2275 A2296 A2298	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone Xs Max	A1921 A2101 A2102 A2103 A2104	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984 A2105 A2106 A2107 A2108	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone X	A1865 A1901 A1902 A1903	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8	A1863 A1905 A1906 A1907	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 7	A1660 A1778 A1779 A1780	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 6S Plus	A1634 A1687 A1690 A1699	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone 6s	A1633 A1688 A1691 A1700	iOS	A9	802.11a/b/g/n/ac	4.2

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone SE	A1662 A1723 A1724	iOS	A9	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (4th gen)	A2229 A2232 A2069 A2233	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 11” (2nd gen)	A2228 A2068 A2230 A2331	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 12.9-inch (3rd gen)	A1876 A1895 A1983 A2014	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Pro 11-inch	A1980 A1934 A1979 A2013	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Air (3rd gen)	A2123 A2152 A2153 A2154	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad mini (5th gen)	A2124 A2125 A2126 A2133	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad Pro (12.9-inch 2nd gen)	A1670 A1671 A1821	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad (7th gen)	A2197 A2198 A2199 A2200	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad (6th gen)	A1893 A1954	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad Pro (12.9)	A1584 A1652	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad (5th gen)	A1822 A1823	iPadOS	A9	802.11a/b/g/n/ac	4.2

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPad Air 2	A1566 A1567	iPadOS	A8X	802.11a/b/g/n/ac	4.2
iPad mini 4	A1538 A1550	iPadOS	A8	802.11a/b/g/n	4.2

Table 2 IT Environment Components

1.3.2 Physical Boundaries

The TOE is a software application running on a mobile device (as listed above). The mobile device platform provides a host Operating System, controls that limit application behavior, and wireless connectivity.

1.3.3 Logical Boundaries

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

1.3.3.1 Cryptographic Support

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

1.3.3.2 User Data Protection

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

1.3.3.3 Security Management

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

1.3.3.4 Privacy

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

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

1.3.3.5 Protection of the TSF

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

1.3.3.6 Trusted Path/Channels

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

1.3.4 TOE Documentation

- Apple iOS and iPadOS 13 Safari Security Target, Version 1.1 [ST] (This Document)
- Apple iOS and iPadOS 13 Safari Security Target Addendum, Version 1.1 (Proprietary)
- Apple iOS and iPadOS 13 Safari Common Criteria Configuration Guide, Version 1.5 [AGD]

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 extended

2.2 Protection Profile Conformance

This TOE is conformant to:

- Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP]
- Application Software Extended Package for Web Browsers, Version 2.0, dated 16 June 2015 [WEBBROWSEREP]

2.3 Conformance Rationale

This Security Target provides exact conformance to Version 1.3 of the Protection Profile for Application Software and Version 2.0 of the Application Software Extended Package for Web Browsers. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile and Extended Package, performing only operations defined there.

2.3.1 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:

Identifier	Applicable	Exclusion Rationale (if applicable)
0510 – Obtaining random bytes for iOS/macOS	Yes	
0505 – Clarification of revocation testing under RFC6066	Yes	
0498 – Application Software PP Security Objectives and Requirements Rationale	Yes	
0495 – FIA_X509_EXT.1.2 Test Clarification	No	The TOE does not directly invoke X.509 functionality.
0486 – Removal of PP-Module for VPN Clients from allowed with list	Yes	
0473 – Support for Client or Server TOEs in FCS_HTTPS_EXT	No	The TOE uses platform HTTPS, so it does not include FCS_HTTPS_EXT.1.
0465 – Configuration Storage for .NET Apps	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
0445 – User Modifiable File Definition	Yes	
0444 – IPsec selections	Yes	
0437 – Supported Configuration Mechanism	Yes	

Identifier	Applicable	Exclusion Rationale (if applicable)
0435 – Alternative to SELinux for FPT_AEX_EXT.1.3	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
0434 – Windows Desktop Applications Test	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
0427 – Reliable Time Source	Yes	
0416 – Correction to FCS_RBG_EXT.1 Test Activity	Yes	

Table 3 SWAPP Technical Decisions

Identifier	Applicable	Exclusion Rationale (if applicable)
0349 – Update to FPT_MCD_EXT.1.2	Yes	

Table 4 Web Browser EP Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [SWAPP] and [WEBBROWSEREP]. It is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

The following threats are drawn directly from the [SWAPP] and [WEBBROWSEREP].

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
T.FLAWED_ADDON	Web browser functionality can be extended through the integration of third-party utilities and tools. Malicious or vulnerable add-ons could result in attacks against the system. Such attacks can allow unauthorized access to sensitive information in the browser, unauthorized access to the platform's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.
T.SAME-ORIGIN_VIOLATION	Violating the same-origin policy is a specialized type of network attack (covered generally as T.NETWORK_ATTACK in the App PP) which involves web content violating access control policies enforced by a web browser to separate the content of different web domains. It is specifically identified as a threat to web browsers, since they implement the access control policies that are violated in these attacks. Attacks which involve same origin violations include: • Insufficient protection of session tokens can lead to session hijacking, where a token is captured and reused in order to gain the privileges of the user who initiated the session. • Cross-site scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks are methods used to compromise user credentials (usually by stealing the user's session token) to a web site. These attacks are more likely a result of server security problems, but some browsers incorporate technologies that try to detect the attacks. • Inadequate sandboxing of browser windows/tabs or a faulty cross domain communications model can lead to leakage of content from one domain in one window/tab to a different domain in a different window/tab. Such attacks leverage the ability of browsers to display content from multiple domains simultaneously.

Table 5 Threats

3.2 Assumptions

The following assumptions are drawn directly from the [SWAPP].

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

Table 6 Assumptions

3.3 Organizational Security Policies

There are no OSPs for the application.

4 Security Objectives

The security objectives have been taken from [SWAPP] and [WEBBROWSEREP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The following security objectives for the TOE were drawn directly from the [SWAPP] and [WEBBROWSEREP].

ID	TOE Objective
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options. Addressed by: FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1, FPT_DNL_EXT.1, FPT_MCD_EXT.1
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs. Addressed by: FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII. Addressed by: FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1, FPR_ANO_EXT.1, FDP_TRK_EXT.1, FMT_MOF_EXT.1
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data. Addressed by: FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1, FDP_COO_EXT.1, FDP_PST_EXT.1
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application. Addressed by: FTP_DIT_EXT.1, FCS_RBG_EXT.1, FCS_CKM_EXT.1, FCS_HTTPS_EXT.1, FDP_NET_EXT.1, FDP_STR_EXT.1

ID	TOE Objective
O.DOMAIN_ISOLATION	To address the network attack associated with content leakage between different web domains, the browser must ensure that content originating from different domains (e.g., in a tab or iFrame) is properly isolated. Addressed by: FDP_ACF_EXT.1.1, FDP_SBX_EXT.1, FDP_SOP_EXT.1
O.ADDON_INTEGRITY	To address issues associated with malicious or flawed add-ons, conformant browsers implement mechanisms to ensure their integrity. This includes verification and validation at installation time and update. Addressed by: FPT_AON_EXT.1, FPT_AON_EXT.2

Table 7 Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. They were drawn directly from the [SWAPP] and track with the assumptions about the environment.

ID	Objective for the Operation Environment
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Table 8 Objectives for the environment

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 and all international interpretations.

Requirement	Description
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_CKM_EXT.1	Cryptographic Key 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_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
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
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_MOF_EXT.1	Management of Functions Behavior
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_AON_EXT.1	Support for Only Trusted Add-ons
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_DNL_EXT.1	File Downloads
FPT_MCD_EXT.1	Mobile Code
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_IDV_EXT.1	Software Identification and Versions
FTP_DIT_EXT.1	Protection of Data in Transit

Table 9 SFRs

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;

- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3);
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 Security Functional Requirements

5.2.1 Cryptographic Support (FCS)

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [

- *invoke platform-provided DRBG functionality,*

] for its cryptographic operations.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [

- *generate no asymmetric cryptographic keys,*

].

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [

- *invoke the functionality provided by the platform to securely store [username/password combinations] ,*

] to non-volatile memory.

5.2.2 User Data Protection (FDP)

FDP_ACF_EXT.1 Local and Session Storage Separation

FDP_ACF_EXT.1.1

The browser shall separate local (permanent) and session (ephemeral) storage based on domain, protocol and port:

- Session storage shall be accessible only from the originating window/tab;
- Local storage shall only be accessible from windows/tabs running the same web application.

FDP_COO_EXT.1 Cookie Blocking

FDP_COO_EXT.1.1

The browser shall provide the capability to block the storage of third party cookies by websites.

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [

- *network connectivity,*
- *camera,*
- *microphone,*
- *location services,*

].

FDP_DEC_EXT.1.2

The application shall restrict its access to [

- *[Keychain],*

] .

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- *user-initiated communication for [accessing websites],*

] .

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [

- *leverage platform-provided functionality to encrypt sensitive data,*

] in non-volatile memory.

FDP_SBX_EXT.1 Sandboxing of Rendering Processes

FDP_SBX_EXT.1.1

The browser shall ensure that web page rendering is performed in a process that is restricted in the following manner:

- The rendering process can only directly access the area of the file system dedicated to the browser.
- The rendering process can only directly invoke inter-process communication mechanisms with its own browser processes.
- The rendering process has reduced privilege with respect to other browser processes [*in no other ways*]

FDP_SOP_EXT.1 Same Origin Policy

FDP_SOP_EXT.1.1

The browser shall only permit scripts contained in one web page to access data in a second web page if both pages are from the same origin.

FDP_SOP_EXT.1.2

The browser shall enforce the same origin policy for all domains.

FDP_STR_EXT.1 Secure Transmission of Cookie Data

FDP_STR_EXT.1.1

The browser shall ensure that cookies containing the *secure* attribute in the set-cookie header are sent over HTTPS.

FDP_TRK_EXT.1 Tracking Information Collection

FDP_TRK_EXT.1.1

The browser shall provide notification to the user when tracking information for [

- *geolocation,*

] is requested by a website.

5.2.3 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall [

- invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.].

FMT_MOF_EXT.1 Management of Functions Behavior

FMT_MOF_EXT.1.1

The browser shall be capable of performing the following management functions, controlled by the administrator or user as shown:

- X = Mandatory
- O = Optional

Management Function	Administrator	User
Enable/disable storage of third party cookies	O, N	X, I
Enable/disable use of OCSP for obtaining the revocation status of X.509 certificates	O, N	O, N
Configure inclusion of user-agent information in HTTP headers	O, N	O, N
Enable/disable ability for websites to collect tracking information about the user through [*[Cookies, Do Not Track requests, location services]*]	O, N	O, I
Enable/disable deletion of stored browsing data (cache, web form information)	O, N	X, I
Enable/disable storage of sensitive information (e.g., auto-fill, auto-complete) in persistent storage	O, N	O, N
Configure size of cookie cache	O, N	O, N
Configure size of cache	O, N	O, N
Enable/disable interaction with Graphic Processing Units (GPUs)	O, N	O, N

Management Function	Administrator	User
Configure the ability to advance to a web site with an invalid or unvalidated X.509 certificate	O, N	O, N
Enable/disable establishment of a trusted channel if the browser cannot establish a connection to determine the validity of a certificate	O, N	O, N
Configure the use of an application reputation service to detect malicious applications prior to download	O, N	O, I
Configure the use of a URL reputation service to detect sites that contain malware or phishing content	O, N	O, I
Enable/disable automatic installation of software updates and patches	O, N	O, N
Enable/disable ability for websites to register protocol handlers	O, N	O, N
Enable/disable display notification when unsigned, untrusted or unverified mobile code is encountered	O, N	O, N
Enable/disable user's ability to select default actions upon download of a file (e.g., always open, or always save, a downloaded file)	O, N	O, N
Enable/disable launching of downloaded files outside the browser	O, N	O, N
Enable/disable JavaScript	O, N	O, I
Enable/disable [*[no mobile code types]*] mobile code	O, N	O, N
Enable/disable support for add-ons	O, N	O, N
Enable/disable individual add-ons	O, N	O, N
Enable/disable HSTS mode	O, N	O

Table 10 Management Functions

Application Note: Implementation of the optional functionality above has been identified as either implemented with an “I” or not implemented with an “N”

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- *[management functions defined in FMT_MOF_EXT.1]*

] .

5.2.4 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1

The application shall [

- *not transmit PII over a network ,*

] .

5.2.5 Protection of TSF (FPT)

FPT_AON_EXT.1 Support for Only Trusted Add-ons

FPT_AON_EXT.1.1

The browser shall include the capability to load [*no add-ons*] .

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [*none*].

FPT_AEX_EXT.1.2

The application shall [

- *not allocate any memory region with both write and execute permissions ,*

] .

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

FPT_DNL_EXT.1 File Downloads

FPT_DNL_EXT.1.1

The browser shall prevent downloaded content from launching automatically.

FPT_DNL_EXT.1.2

The browser shall present the user with the option to either save or discard downloaded files.

FPT_MCD_EXT.1 Mobile Code

FPT_MCD_EXT.1.1

The browser shall support the capability to execute signed [

- *no*

] mobile code.

FPT_MCD_EXT.1.2

The browser shall [*automatically discard*] unsigned, untrusted or unverified [

- *[all mobile code types]*

] mobile code without executing it.

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

The application shall [*leverage the platform*] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2

The application shall **[***leverage the platform*] to query the current version of the application software.

FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4

The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5

The application is distributed [*with the platform OS*]

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [*none*].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [*[Bundle configuration information (bundle ID and version number)]*] .

5.2.6 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [

- *invoke platform-provided functionality to encrypt all transmitted data with [HTTPS, TLS]*

] between itself and another trusted IT product.

5.3 Dependency Rationale for SFRs

The Security Target contains all of the required SFRs from the Protection Profile for Application Software and Application Software Extended Package for Web Browsers. Based on the instructions contained in the PP and EP, the Security target includes all required selection-based SFRs. The dependency analysis can be found within the PP and EP. As such, the dependencies are not applicable since the PP and EP have been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Protection Profile for Application Software and Common Criteria Part 3 Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_TSU_EXT.1	Timely Security Updates
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

Table 11 Security Assurance Requirements

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Apple to satisfy the assurance requirements. The table below lists the details.

SAR	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and

SAR	How the SAR will be met
	error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ALC_TSU_EXT.1	Apple uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure.
ATE_IND.1	Apple will provide the TOE for testing.
AVA_VAN.1	Apple will provide the TOE for testing.

Table 12 TOE Security Assurance Measures

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

SFR	Rationale
FCS_RBG_EXT.1	The TOE leverages the platform provided SecRandomCopyBytes for random bit services. Specifically, the TOE uses the random bits to generate UUIDs for each tab. The UUIDs are used to support process separation in FDP_SBX_EXT.1.
FCS_CKM_EXT.1	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.
FCS_STO_EXT.1	The TOE allows the user to save usernames and passwords used to login to websites in the Keychain (i.e. platform provide credential store).
FDP_ACF_EXT.1	The TOE runs in a sandbox environment within the underlying platform OS. The TOE does not access to storage outside of the implemented sandbox. The storage used by the TOE is isolated from the underlying platform. 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.
FDP_COO_EXT.1	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.
FDP_DEC_EXT.1	The TOE requests only access to the following hardware resources: • Network connectivity • Camera • Microphone • Location services The TOE does not access any sensitive information repositories.
FDP_NET_EXT.1	The TOE communicates on the network (accessing external websites) based upon user-initiated actions.
FDP_DAR_EXT.1	During operation of the TOE, any sensitive information stored securely is protected by platform-provided functionality to encrypt the sensitive data. All user requested browser information (autofill information) stored on the platform is stored under Class A (Complete Protection). No other files are stored by the application.
FDP_SBX_EXT.1	The TOE is a first-party application provided as part of the underlying platform. The TOE renders HTML and interprets JavaScript for each tab in a separate process. The process for each tab calls the underlying platform's libraries to process the request (continuing to execute in the context of the calling process). 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.

SFR	Rationale
FDP_SOP_EXT.1	Each browser tab/window is individually isolated from the other open tabs and does not allow data to flow between tabs. No exceptions made due to the state or condition of the tab. Each tab/window requires appropriate adherence to the authentication requirements and restrictions. Cookies are considered persistent data and are shared between tabs as described in FDP_ACF_EXT.1, subject to the same origin policy. The TOE's implementation of the same origin policy is fully compliant with RFC 6454; the same origin policy is applied to all web browser tab/windows independently. There are not any situations where conformance is relaxed.
FDP_STR_EXT.1	In accordance with RFC 6265, the TOE supports the use of the 'secure' attribute within the set-cookie header. Cookies that are sent over HTTPS are required to contain this attribute within the header. Cookies with the 'secure' attribute are not sent over plaintext HTTP connections.
FDP_TRK_EXT.1	The TOE provides notifications to users when a request for geolocation is received from a website. The request is displayed as a pop-up to the user and offers the option to allow or deny the request.
FMT_MEC_EXT.1	The TOE maintains a restricted configuration with no management functions being performed by users. All configuration options are stored and set by the underlying platform. The TOE reads configuration options from platform's user defaults system.
FMT_MOF_EXT.1 FMR_SMF.1	The TOE allows the user to perform several managements functions including, • Enabling and disabling storage of cookies • Enabling and disabling the ability for websites to collect tracking information • Deletion of stored browsing data • Enabling and disabling storage of autofill and auto-complete data • Configuring the use of an application reputation service to detect malicious applications prior to download • Configuring the use of a URL reputation service to detect sites that contain malware or phishing content • Enabling and disabling JavaScript Each of these settings is provided through the underlying Platform. The TOE does not provide a separate configuration interface. Each of these settings are stored in the user defaults system by the underlying platform.
FMT_CFG_EXT.1	The TOE does not come with any default credentials. The user must configure an account first before accessing the TOE and underlying platform. As described in FDP_DAR_EXT.1, all data stored by the TOE is stored under Class C.
FPR_ANO_EXT.1	The TOE does not specifically request PII from the user. Any information provided by the user is entered without prompting from the TOE.
FPT_AON_EXT.1	The TOE is not capable of loading trusted add-ons, because the TOE does not support the use of add-ons.
FPT_API_EXT.1	The following API frameworks are used by Safari: • Accounts.framework • AuthenticationServices.framework • CFNetwork.framework • Contacts.framework • ContactsUI.framework • CoreFoundation.framework

SFR	Rationale
	• CoreGraphics.framework • CoreLocation.framework • CoreMedia.framework • CoreServices.framework • CoreSpotlight.framework • CoreTelephony.framework • CoreText.framework • DocumentManagerCore.framework • Foundation.framework • Intents.framework • ImageIO.framework • IOKit.framework • JavaScriptCore.framework • LinkPresentation.framework • LocalAuthentication.framework • MapKit.framework • MediaPlayer.framework • MobileCoreServices.framework • OnBoardingKit.framework • QuartzCore.framework • SafariServices.framework • Security.framework • TextInput.framework • UIKit.framework • WebKit.framework
FPT_AEX_EXT.1	The TOE is compiled with ASLR enabled (achieved by compiling with the -fPIE flag). The TOE does not request any memory mappings with the write and execute permissions The TOE does not make any calls to mmap or mprotect. The underlying platform is iOS or iPadOS, so the platform ensures the TOE: 1) is compatible with the platform security features 2) writes data to the application working directory and not the directory containing executable files The TOE is compiled with stack-based buffer overflow protection enabled (achieved by compiling with the -fstack-protector-all flag).
FPT_DNL_EXT.1	The TOE does not permit automatic downloading of from a website. The content 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 TOE does not launch downloaded content automatically.
FPT_MCD_EXT.1	The TOE does not support any types of mobile code.
FPT_TUD_EXT.1	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 current versions of the TOE can be checked through the Settings of the underlying platform.

SFR	Rationale
FPT_LIB_EXT.1	The TOE does not leverage any third-party libraries. It is a first-party application that is provided on the underlying platform by the vendor.
FPT_IDV_EXT.1	Each iOS and iPadOS application must be distributed in as an Application Bundle. Each Bundle is required to include a bundle ID and version number. These are the CFBundleIdentifier and CFBundleShortVersionString values respectively in the Info.plist file.
FTP_DIT_EXT.1	All application data is transmitted securely via HTTPS and TLS. The TOE invokes the platform provided HTTPS/TLS using the NSURLSession class. The TOE transmits HTML form data which may contain credentials; however, the TOE does not request or use credentials for its operation.
ALC_TSU_EXT.1	To report security or privacy issues that affect Apple products or web servers, should contact product-security@apple.com. Submissions can use Apple's Product Security PGP key (https://support.apple.com/en-us/HT201214) to encrypt sensitive information that is sent by email. When the email is received, Apple will send an automatic email as acknowledgment. If this email is not received, please check the email address and send again. For the protection of our customers, Apple generally does not disclose, discuss, or confirm security issues until a full investigation is complete and any necessary patches or releases are available. Apple distributes information about security issues in its products through security advisories. Users can also receive Apple security advisories through the security-announce mailing list.

Table 13 TOE Summary Specification SFR Description