Apple Inc.

Apple iOS 12 Safari on iPhone and iPad Common Criteria Configuration Guide

June 2019

Version 1.1

Contents

Revision History

Version	Date	Description
1.0	March 2019	Initial Version
1.1	June 2019	Updated based on Safari version change.

1 Introduction

1.1 Target of Evaluation

The TOE is the Apple iOS 12 Safari on iPhone and iPad. 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 operating system has been separately validated (VID 10937). The evaluated version of the TOE is version 12.3.1.

Table 1 – Evaluated Platforms				
Device Name	**Model**	**Processor**	**WiFi**	**Bluetooth**
iPhone XS	A1920 A2097 A2098 A2099 A2100	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XS Max	A1921 A2101 A2102 A2103 A2104	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984 A2105 A2106 A2107 A2108	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone X	A1901 A1902 A1865	A11	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	5.0
iPhone 8 Plus/ iPhone 8	A1864, A1897, A1898, A1899/ A1863, A1905, A1906, A1907	A11	802.11a/b/g/n/ac 802.11a/b/g/n/ac	5.0
iPhone 7 Plus/ iPhone 7	A1661, A1784, A1785, A1786/ A1660, A1778, A1779, A1780	A10	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPhone 6S Plus/ iPhone 6S	A1634, A1687, A1690, A1699/ A1633, A1688, A1691, A1700	A9	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPhone SE	A1662 A1723 A1724	A9	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2
iPhone 6 Plus/ iPhone 6	A1522, A1524, A1593/ A1549, A1586, A1589	A8	802.11a/b/g/n/ac 802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.0 4.0 4.0
iPad mini 4	A1538 A1550	A8	802.11a/b/g/n 802.11a/b/g/n	4.2 4.2
iPad Air 2	A1566 A1567	A8X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad (5th gen)	A1822 A1823	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2

iPad Pro 12.9" (1st Gen)	A1584 A1652	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 9.7"	A1673 A1674	A9X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 12.9" (2nd Gen)	A1670 A1671	A10X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad Pro 10.5"	A1701 A1709	A10X	802.11a/b/g/n/ac 802.11a/b/g/n/ac	4.2 4.2
iPad 9.7"	A1893 A1954	A10	802.11a/b/g/n/ac	4.2

Table 1 TOE Platforms

1.2 Document Purpose and Scope

This document describes the installation and Common Criteria evaluation related usage of the Apple iOS 12 Safari on iPhone and iPad.

This guide will show you how to install and operate the software in a Common Criteria compliant manner. You will learn:

- How to verify the app version
- The secure communication mechanisms employed by the TOE
- How to configure user data and self-protection features
- Platform resources used by the TOE
- Evaluated functionality
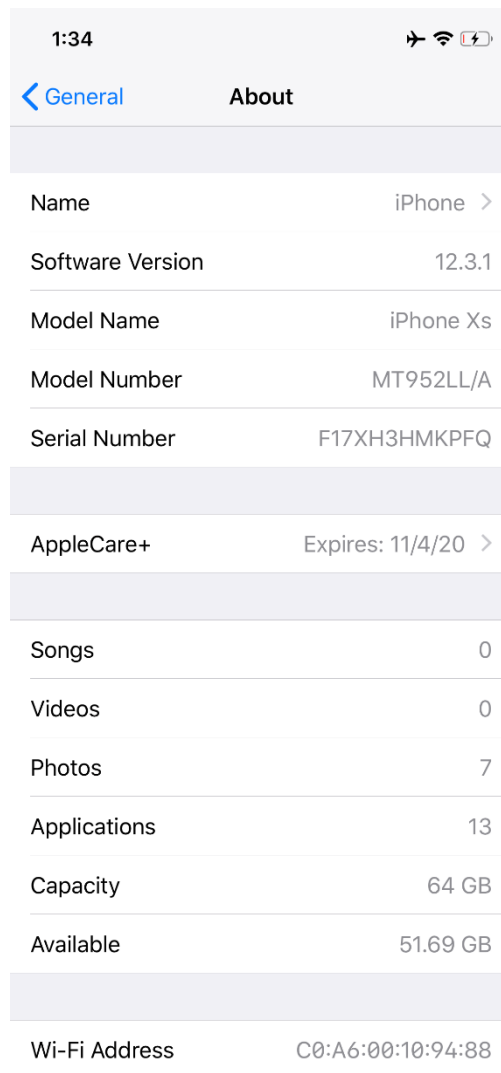
2 Installation/Update

The Safari App is loaded by default on the Common Criteria evaluated version of Apple iOS (VID 10937). It is not possible to delete Safari as it is a core OS application. All updates to it are released via OS update. All applications found on the Apple App Store are digitally signed.

2.1 Verifying Product Version

The Apple iOS 12 Safari is a core OS application. These applications are not updated separately from iOS and are versioned identically to the OS. The following steps are followed in order to verify the application (and OS version).

- Tap the "Settings" application in iOS
- Tap the "General" option
- Tap the "About" option

The following is an example of this verification,

1:34	✈ 🛜 🔋
‹ General	**About**
Name	iPhone ›
Software Version	12.3.1
Model Name	iPhone Xs
Model Number	MT952LL/A
Serial Number	F17XH3HMKPFQ
AppleCare+	Expires: 11/4/20 ›
Songs	0
Videos	0
Photos	7
Applications	13
Capacity	64 GB
Available	51.69 GB
Wi-Fi Address	C0:A6:00:10:94:88

If a new version of the OS/TOE are available, it will be indicated on this screen.

2.2 Other Assumptions

In order to use the TOE in the evaluated configuration, the TOE Platform (i.e., the iPhone or iPad) must also be configured to meet the requirements of the Protection Profile for Mobile Device Fundamentals Version 3.1 as set forth in the Security Target and guidance documentation for the Apple iOS 12 software (https://niap-ccevs.org/Product/Compliant.cfm?PID=10937), operating on one of the hardware platforms listed in Table 1.

3   Cryptographic Support

3.1 TLS Configuration

The Apple iOS 12 Safari on iPhone and iPad application supports secure communications with websites via HTTPS/TLS. In support of these communications, the following Ciphersuites are supported,

- TLS_RSA_WITH_AES_128_CBC_SHA256,
- TLS_RSA_WITH_AES_256_CBC_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Additionally, the following Elliptic Curve Extensions are supported,

- secp256r1,
- secp384r1.

All configuration of these connections is handled exclusively by the underlying platform (Apple iOS). No additional configuration is required to ensure proper usage.

3.2 Digital Certificates

The Apple iOS 12 Safari on iPhone and iPad application leverages "Trusted" digital certificates installed in the iOS Trust Store. No configuration is required to facilitate the usage of these digital certificates. Additional information regarding the Apple iOS 12 Trust Store may be found at: https://support.apple.com/en-us/HT209144

The Apple iOS 12 Safari on iPhone and iPad application automatically uses the domain name of the server being contacted as the reference identifier. Again, no configuration is required.

To manually install trust certificates, refer to https://support.apple.com/en-us/HT204477.

4   Resource Usage

The Apple iOS 12 Safari on iPhone and iPad application uses the following resources,

- Network Connectivity: This is required for the TOE 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.

5   User Data Protection

5.1 Local and Session Storage Separation

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. This data is only store in physical memory assigned to the browser tab.

- Local storage shall only be accessible from windows/tabs running the same web application. This data is store in the dedicated browser sandbox.

No configuration is required to enforce this behavior.

5.2 Sandboxing of Rendering Processes

The browser ensures 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 no other privilege with respect to other browser processes.

No configuration is required to enforce this behavior.

5.3 Tracking Information Collection

The browser shall provide notification to the user when tracking information for geolocation or browser preferences are requested by a website. The following is an example,
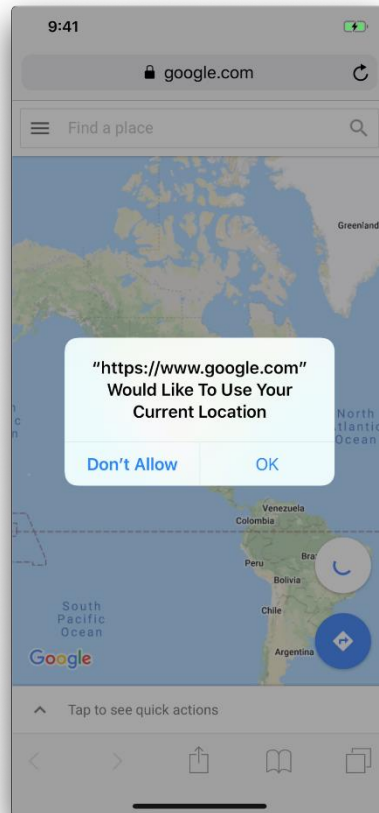
No configuration is required to enforce this behavior.

## 5.4 Cookie Blocking and Other Tracking Behavior & Security Features

Use the following configurations to enable or disable security features of the TOE.

- To enable/disable storage of third-party cookies, tap Settings > Safari > Block All Cookies.
- To prevent websites from tracking you, tap Settings > Safari > Ask Websites Not to Track Me.
- To prevent cross-site tracking, tap Settings > Safari > Prevent Cross-Site Tracking.
- To clear your history and cookies, tap Settings > Safari > Clear History and Website Data. Clearing your history, cookies, and browsing data from Safari won't change 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.

6 Self-Protection

6.1 File Downloads

The browser shall prevent downloaded content from launching automatically. Whenever a file is presented for download, a dialog box is presented. The file will not download without explicit user action. The following is an example of such dialog box:
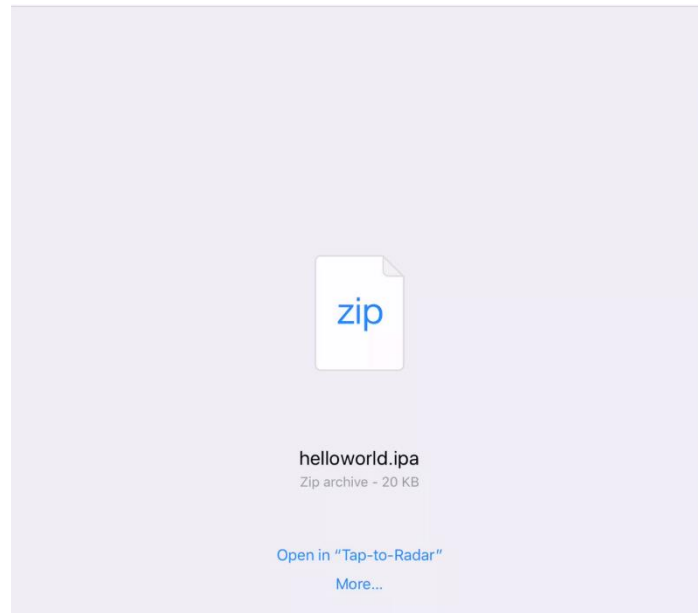
No configuration is required to enforce this behavior.

6.2 Mobile Code

The browser shall support the capability to execute signed *JavaScript* mobile code. If the browser is presented unsigned, untrusted, or unverified JavaScript, the code is discarded and not executed.

No configuration is required to enforce this behavior.

6.3 Support for Add-ons

The TOE does not support add-ons.

7 Evaluated Functionality

In addition to the base functionality found in the Protection Profile for Application Software, the following functionality was also evaluated for the Apple iOS 12 Browser on iPhone and iPad application.

- Application Software Extended Package for Web Browsers

End of Document