Common Criteria SWAPP and WEBBROWSEREP Assurance Activity Report Apple iOS 12 Safari

Acumen Security

ISSUED BY

Acumen Security, LLC.

Revision History:

Version	Date	Changes
Version 0.1	March 2019	Initial Draft
Version 1.0	June 2019	Updated to address ECR comments

Table of Contents

Assurance Activity Report (AAR) for a Target of Evaluation

Apple iOS 12 Safari

Apple iOS 12 Safari Security Target version 1.0
Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP]
Extended Package for Web Browsers, version 2.0, dated 16 June 2015 [WEBBROWSEREP]

Evaluated by:

2400 Research Blvd. #395
Rockville, MD 20850

Prepared for:
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
Danielle F Canoles
Rutwij Kulkarni
Rodrigo Tapia

Common Criteria Version
Common Criteria Version 3.1 Revision 4

Common Evaluation Methodology Version
CEM Version 3.1 Revision 4

1 TOE Overview

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

Note: The TOE is the Safari software only. The Apple iOS operating system has been separately validated (VID 10937).

1.1 TOE Description

The TOE is an application on a mobile operating system. The TOE is the Safari browser application only. The Apple iOS operating system has been separately validated (VID 10937). The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 12.3.1.

As evaluated, the TOE software runs on the following devices

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 5.0 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 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 4.2 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

The Operating System on which the TOE is running is Apple iOS version 12. This is the same version of iOS which has undergone Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals Version 3.1.

2 Security Functional Requirement Identification

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

Table 2 – Included SFRs	
Requirement	**Auditable Event**
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.4	TLS Client Protocol
FDP_ACF_EXT.1	Local and Session Storage Separation
FDP_COO_EXT.1	Cookie Blocking
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
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
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_MOF_EXT.1	Management of Functions Behavior
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Info
FPT_AON_EXT.1	Support for Only Trusted Addons
FPT_DNL_EXT.1	File Downloads
FPT_MCD_EXT.1	Mobile Code
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_TUD_EXT.1	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

3 Test Equivalency Justification

3.1 Architectural Description of the TOE

The TOE is an application on a mobile operating system. When deployed, the TOE provides secure communications to remote users outside of an organizations protected network. The evaluated version of the TOE is version 12.3.1.

3.2 Processor Analysis

The platforms on which the TOE resides contain one of eight processors, including,

- Apple A12
- Apple A11
- Apple A10X
- Apple A10
- Apple A9X
- Apple A9
- Apple A8X
- Apple A8

While architecturally similar, each of the processor do contain differences. Because of this, it is recommended that testing be performed on each processor.

3.3 Software/OS Dependencies Analysis

The underlying OS is installed on each of the platforms on which the TOE resides. The underlying OS for all models within the TOE is iOS version 12. There are no specific dependencies on the OS since the TOE will not be installed on different OSs

3.4 Differences in Libraries Used to Provide TOE Functionality Analysis

All software binaries compiled in the TOE software are identical including the version of the library. There are no differences between the included libraries. Because the OS is identical on each of the tested platforms, there are no differences in the libraries on the platforms themselves.

3.5 TOE Functional Differences Analysis

The TOE is a single software tested on a single version of an OS on multiple platforms. Regardless of the platform on which the TOE is running, the provided functionality is the same.

3.6 Test Subset Justification/Rationale

Based on these analyses above, it is recommended that the TOE be tested on an example of a platform running an Apple A8, Apple A8X, Apple A9, Apple A9X, Apple A10, Apple A10X, Apple A11 and Apple A12. The following will be used for testing,

Table 3 – Test Subset

Device	CPU Model	Operating System
iPhone 6 Plus	A8	Apple iOS 12
iPad Air 2	A8X	Apple iOS 12
iPhone 6S Plus	A9	Apple iOS 12

iPad Pro 9.7	A9X	Apple iOS 12
iPhone 7	A10	Apple iOS 12
iPad Pro	A10X	Apple iOS 12
iPhone 8 Plus	A11	Apple iOS 12
iPhone XS	A12	Apple iOS 12
iPhone XS Max	A12	Apple iOS 12
iPhone XR	A12	Apple iOS 12

Due to publicly know vulnerabilities in version 12, the TOE was updated to version 12.3.1. Regression testing was performed to verify SFRs related to the updated functionality remained unchanged.

4 Platform Test Result Reuse

All Apple application leverage a series of functional frameworks to provide common functionality across applications. Much of this functionality was directly tested as part of the iOS platform evaluation (VID 10937). In Support of data reuse and to facilitate meaningful efficient testing, it was agreed by NIAP that it would be allowable to directly leverage previously reviewed/vetted platform testing for services that used platform functionality included in VID 10937. The following test cases, reused output from platform testing and were not re-run as part of this evaluation.

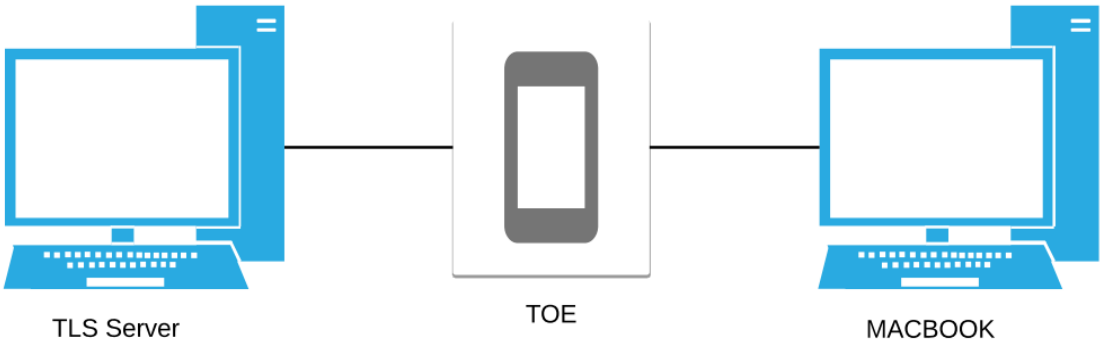
- FCS_TLSC_EXT.1.1 Test #1
- FCS_TLSC_EXT.1.1 Test #2
- FCS_TLSC_EXT.1.1 Test #3
- FCS_TLSC_EXT.1.1 Test #4
- FCS_TLSC_EXT.1.1 Test #5 (1) - (6)
- FCS_TLSC_EXT.1.2 Test #1
- FCS_TLSC_EXT.1.2 Test #2
- FCS_TLSC_EXT.1.2 Test #3
- FCS_TLSC_EXT.1.2 Test #4
- FCS_TLSC_EXT.1.2 Test #5 (1) - (3)
- FCS_TLSC_EXT.1.3 Test #1
- FCS_TLSC_EXT.4 Test #1
- FCS_HTTPS_EXT.1.1 Test #1
- FCS_HTTPS_EXT.1.2 Test #1
- FCS_HTTPS_EXT.1.3 Test #1
- FIA_X509_EXT.1.1 Test #1
- FIA_X509_EXT.1.1 Test #2
- FIA_X509_EXT.1.1 Test #3
- FIA_X509_EXT.1.1 Test #4
- FIA_X509_EXT.1.1 Test #5
- FIA_X509_EXT.1.1 Test #6
- FIA_X509_EXT.1.1 Test #7
- FIA_X509_EXT.1.2 Test #1
- FIA_X509_EXT.1.2 Test #2
- FIA_X509_EXT.1.2 Test #3
- FIA_X509_EXT.2.2 Test #1
- FIA_X509_EXT.2.2 Test #2

This is reflected in the note section of each of the applicable test cases.

5 Test Diagram

5.1 Testbed Diagram

Below is a visual representation of the components included in the test bed:



5.2 Configuration Information

The following provides configuration information about each device on the test network.

5.2.1 *TOE*

- OS: Apple iOS 12
- TOE: Apple iOS 12 Safari

5.2.2 *TLS Server*

- Application: OpenSSL

5.2.3 *Mac Book*

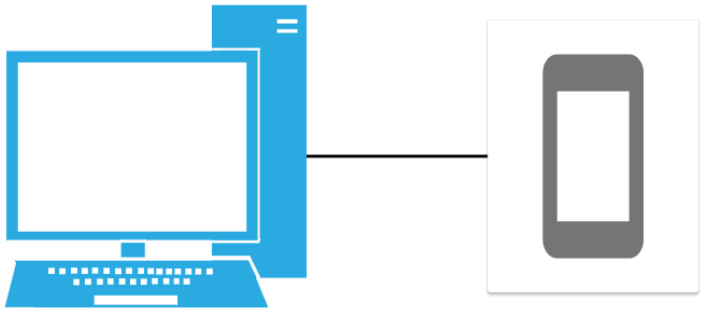
- Application: OpenSSH

5.2.4 *TOE Testing Timeframe and Location*

- The TOE specific testing was conducted during the timeframe of October 2018 through January 2019.
- The TOE specific testing was conducted at Acumen Security CCTL located at Rockville, MD and Apple Inc. Reston facilities located at Reston, VA.

5.3 Testbed Diagram (Platform Testbed)

Below is a visual representation of the components included in the test bed:



5.4 Configuration Information

The following provides configuration information about each device on the test network.

5.4.1 *TOE Platform*

- OS: Apple iOS 12

5.4.2 *TLS Server*

- Application: OpenSSL

5.4.3 *Platform Testing Timeframe and Location*

- Platform testing was conducted September 17-21, 2018
- Platform testing was conducted at Apple Inc. headquarters in Cupertino, CA

6 Detailed Test Cases

6.1 Test Cases (Cryptographic Support)

6.1.1 *FCS_HTTPS_EXT.1.1 Test 1*

Table 4 – FCS_HTTPS_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FCS_HTTPS_EXT.1.1_T1
Objective	The evaluator shall attempt to establish an HTTPS connection with a webserver, observe the traffic with a packet analyzer, and verify that the connection succeeds and that the traffic is identified as TLS or HTTPS.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Attempt to establish an HTTPS connection with a server • Observe the traffic with a packet analyzer • Verify that the connection succeeds and that the traffic is identified as TLS or HTTPS
Pass/Fail Explanation	HTTPS/TLS is used for connections. This meets the testing requirements.
Result	Pass

6.1.2 *FCS_HTTPS_EXT.1.2 Test 1*

Table 5 – FCS_HTTPS_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FCS_HTTPS_EXT.1.2_T1
Objective	Other tests are performed in conjunction with FCS_TLSC_EXT.1 and/or FCS_TLSS_EXT.1.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Pass/Fail Explanation	See FCS_TLSC_EXT.1 for details of testing. All tests successfully completed. This meets the testing requirements.
Result	Pass

6.1.3 *FCS_HTTPS_EXT.1.3 Test 1*

Table 6 – FCS_HTTPS_EXT.1.3 Test 1	
Item	**Data/Description**
Test ID	FCS_HTTPS_EXT.1.3_T1
Objective	The evaluator shall demonstrate that using a certificate without a valid certification path results in the selected action in the SFR. If "notify the user" is selected in the SFR, then the evaluator shall also determine that the user is notified of the certificate validation failure. Using the administrative guidance, the evaluator shall then load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that again, using a certificate without a valid certification path results in the selected action in the SFR,

	and if "notify the user" was selected in the SFR, the user is notified of the validation failure.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Determine that the user is notified of the certificate validation failure • Load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function • Demonstrate that the function succeeds • Delete one of the certificates, and show that again, using a certificate without a valid certification path results in notification
Pass/Fail Explanation	When a valid certificate chain is present certificate validation succeeds. When a valid certificate chain is not present, certificate validation fails. This meets the testing requirements.
Result	Pass

6.1.4 *FCS_RBG_EXT.1.1 TSS*

Table 7 – FCS_RBG_EXT.1.1 TSS	
The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below. For iOS: The evaluator shall verify that the application invokes SecRandomCopyBytes or uses /dev/random directly to acquire random.	
Evaluator Findings	The evaluator examined the TSS and confirmed that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the random numbers obtained from the platform are used to generate UUIDs for each tab. The UUIDs are used to support process separation in FDP_SBX_EXT.1. Next, the evaluator determined that for this function, the TSS states which platform interface (API) is used to obtain the random numbers. Specifically, SecRandomCopyBytes is used to generate the required random numbers. The evaluator found this to correspond to the acceptable interface for iOS. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.5 *FCS_STO_EXT.1.1 TSS*

Table 8 – FCS_STO_EXT.1.1 TSS	
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 of the ST was used to determine the verdict of this activity.

	Upon investigation, the evaluator found that the TOE does not store any credentials/keys. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.6 *FCS_STO_EXT.1.1 Test 1*

Table 9 – FCS_STO_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FCS_STO_EXT_1_1_T1
Objective	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.
Pass/Fail Explanation	The Apple iOS 12 Safari Application does not store any credentials. Therefore, there is no credentials to verify. This meets the testing requirements.
Result	Pass

6.1.7 *FCS_TLSC_EXT.1.1 TSS 1*

Table 10 – FCS_TLSC_EXT.1.1 TSS	
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component	
Evaluator Findings	The evaluator examined the description of the implementation of TLS in the TSS to ensure that the cipher suites supported are specified. Section 6 of the ST was used to determine the verdict of this assurance activity. The evaluator found that seven TLS ciphersuites are supported by the TOE. These ciphersuites were found to be consistent with those listed in section 5.2.1 of the ST. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.8 *FCS_TLSC_EXT.1.1 Guidance*

Table 11 – FCS_TLSC_EXT.1.1 Guidance	
The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.	
Evaluator Findings	The evaluator examined AGD to determine that any configuration that is required to be done to configure the functionality for the required modes and key sizes is present. Section 3 of AGD, titled "Cryptographic Support," was used to determine the verdict of this activity. Upon investigation, the evaluator found that AGD discusses the supported TLS algorithms (including elliptic curves). Additionally, the evaluator found that the AGD explicitly states that no configuration is required for proper usage. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.9 *FCS_TLSC_EXT.1.1 Test 1*

Table 12 – FCS_TLSC_EXT.1.1 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T1
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Configure a server to accept one ciphersuite at a time • Connect to the server • Repeat for each ciphersuite • Verify that each specified ciphersuite is present
Pass/Fail Explanation	The TOE supports the claimed TLSC ciphersuites. This meets the testing requirements.
Result	Pass

6.1.10 *FCS_TLSC_EXT.1.1 Test 2*

Table 13 – FCS_TLSC_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T2
Objective	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a certificate missing the Server Authentication purpose in the extendedKeyUsage field • Connect to a server using the certificate • Verify that the connection is rejected
Pass/Fail Explanation	The connection with a TLS server with a malformed server certificate is rejected. This meets the testing requirements.
Result	Pass

6.1.11 *FCS_TLSC_EXT.1.1 Test 3*

Table 14 – FCS_TLSC_EXT.1.1 Test 3	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T3
Objective	The evaluator shall send a server certificate in the TLS connection that does not match the server-selected ciphersuite (for example, send a ECDSA certificate while

	using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite or send a RSA certificate while using one of the ECDSA ciphersuites.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server that sends a server certificate that does not match the server-selected ciphersuite • Verify that a connection is not established
Pass/Fail Explanation	A connection was not established when a server certificate that does not match the server-selected ciphersuite is presented. This meets the testing requirements.
Result	Pass

6.1.12 *FCS_TLSC_EXT.1.1 Test 4*

Table 15 – FCS_TLSC_EXT.1.1 Test 4	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4
Objective	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server that sends a TLS_NULL_WITH_NULL_NULL ciphersuite • Attempt to connect to the server • Verify that a connection is not established
Pass/Fail Explanation	A connection was not established when the TLS_NULL_WITH_NULL_NULL ciphersuite is presented. This meets the testing requirements.
Result	Pass

6.1.13 *FCS_TLSC_EXT.1.1 Test 5*

Table 16 – FCS_TLSC_EXT.1.1 Test 5	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T5
Objective	The evaluator shall perform the following modifications to the traffic: • Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection. • Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message. • Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello. • Modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message.

	• Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data. • Send an garbled message from the Server after the Server has issued the ChangeCipherSpec message and verify that the client denies the connection
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Make various modification to traffic as required • Verify that the client rejects the connection
Pass/Fail Explanation	The modified TLS connection was rejected. This meets the testing requirements.
Result	Pass

6.1.14 *FCS_TLSC_EXT.1.2 TSS*

Table 17 – FCS_TLSC_EXT.1.2 TSS	
The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the application configured reference identifier, including which types of reference identifiers are supported (e.g. Common Name, DNS Name, URI Name, Service Name, or other application¬ specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator shall ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the TOE.	
Evaluator Findings	The evaluator examined the TSS to determine if it describes the client's method of establishing all reference identifiers. Section 6 of the ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states that when the TOE uses the APIs provided by the platform to attempt to establish a trusted channel, the TOE will compare the DN contained within the peer certificate (specifically the Subject CN, as well as any Subject Alternative Name fields, IP Address, or Wildcard certificate if applicable) to the DN of the requested server. If the DN in the certificate does not match the expected DN for the peer, then the application cannot establish the connection. Both IP addresses and wildcards are supported for reference identifiers. Finally, certificate pinning is not supported. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.15 *FCS_TLSC_EXT.1.2 Guidance*

Table 18 – FCS_TLSC_EXT.1.2 Guidance	
The evaluator shall verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.	
Evaluator Findings	The evaluator verified that AGD includes instructions for setting the reference identifier. Upon investigation, the evaluator found that section 3.2 of AGD, titled "Digital Certificates," describes that the TOE leverages "Trusted" digital certificates in the iOS Trust Store and that no configuration of reference identifiers is required. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.16 *FCS_TLSC_EXT.1.2 Test 1*

Table 19 – FCS_TLSC_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T1
Objective	The evaluator shall present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator shall verify that the connection fails.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server that presents a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier • Attempt to connect to the server • Verify that a connection is not established
Pass/Fail Explanation	A connection was not established when presented a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. This meets the testing requirements.
Result	Pass

6.1.17 *FCS_TLSC_EXT.1.2 Test 2*

Table 20 – FCS_TLSC_EXT.1.2 Test 2	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T2
Objective	The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server that presents a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier • Attempt to connect to the server • Verify that a connection is not established
Pass/Fail Explanation	A connection was not established when presented a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. This meets the testing requirements.
Result	Pass

6.1.18 *FCS_TLSC_EXT.1.2 Test 3*

Table 21 – FCS_TLSC_EXT.1.2 Test 3	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T3

Objective	The evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension • Attempt to connect to the server • Verify that a connection is not established
Pass/Fail Explanation	A connection was established when presented server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. This meets the testing requirements.
Result	Pass

6.1.19 *FCS_TLSC_EXT.1.2 Test 4*

Table 22 – FCS_TLSC_EXT.1.2 Test 4	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T4
Objective	The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension • Attempt to connect to the server • Verify that a connection is established
Pass/Fail Explanation	A connection was established when presented server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. This meets the testing requirements.
Result	Pass

6.1.20 *FCS_TLSC_EXT.1.2 Test 5*

Table 23 – FCS_TLSC_EXT.1.2 Test 5	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5
Objective	The evaluator shall perform the following wildcard tests with each supported type of reference identifier. The support for wildcards is intended to be optional. If wildcards are supported, the first, second, and third tests below shall be executed. If wildcards are not supported, then the fourth test below shall be executed. • Test 5.1: [conditional]: If wildcards are supported, the evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails. • Test 5.2: [conditional]: If wildcards are supported, the evaluator shall present a server certificate containing a wildcard in the left-most label but

	not preceding the public suffix (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails. • Test 5.3: [conditional]: If wildcards are supported, the evaluator shall present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator shall configure the reference identifier with a single leftmost label (e.g. foo.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Set up server with a variety of server certificates created to reflect the condition specified in each of the tests • Confirmed that the expected behavior occurs in each case.
Pass/Fail Explanation	The TOE rejects reference identifiers with wildcards that aren't in the left-most position.
Result	Pass

6.1.21 *FCS_TLSC_EXT.1.3 Test 1*

Table 24 – FCS_TLSC_EXT.1.3 Test 1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT_1_3_T1
Objective	The evaluator shall demonstrate that a peer using a certificate without a valid certification path results in an authenticate failure. Using the administrative guidance, the evaluator shall then load the trusted CA certificate(s) needed to validate the peer's certificate, and demonstrate that the connection succeeds. The evaluator then shall delete one of the CA certificates, and show that the connection fails.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Attempt to connect to a peer using a certificate without a valid certification path • This results in an authenticate failure • Load the trusted CA certificate(s) needed to validate the peer's certificate • Demonstrate that the connection succeeds • Delete one of the CA certificates • Show that the connection fails
Pass/Fail Explanation	A connection is made when a full certificate chain is present. A connection is not made when a full certificate chain is not present. This meets the testing requirements.
Result	Pass

6.1.22 *FCS_TLSC_EXT.4.1 TSS*

Table 25 – FCS_TLSC_EXT.4.1 TSS	
The evaluator shall verify that TSS describes the supported Elliptic Curves Extension and whether the required behavior is performed by default or may be configured.	
Evaluator Findings	The evaluator examined the TSS in section 6 of the ST to determine if the supported Elliptic Curves Extensions are described and whether the required behavior is performed by default. Upon investigation, the evaluator found that the TSS of ST states that the following elliptic curves are supported, • secp256r1 • secp384r1 The evaluator also found that these curves are supported by default and no configuration is required. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.23 *FCS_TLSC_EXT.4.1 Guidance*

Table 26 – FCS_TLSC_EXT.4.1 Guidance	
If the TSS indicates that the supported Elliptic Curves Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the supported Elliptic Curves Extension.	
Evaluator Findings	The evaluator used AGD section 3, titled "Cryptographic Support," to determine the verdict of this activity. Upon investigation, the evaluator found that no configuration required which is consistent with the ST. Based on these findings, this Assurance Activity is considered satisfied.
Verdict	Pass

6.1.24 *FCS_TLSC_EXT.4.1 Test 1*

Table 27 – FCS_TLSC_EXT.4.1 Test 1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.4.1_T1
Objective	The evaluator shall configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Configure a server to perform ECDHE key exchange using each of the TOE's supported curves • Verify that the TOE successfully connects to the server
Pass/Fail Explanation	secp256r1 and secp384r1 are supported for TLS connections. This meets the testing requirements.
Result	Pass

6.1.25 *FDP_DEC_EXT.1.1 TSS 1*

Table 28 – FDP_DEC_EXT.1.1 TSS 1

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 reviewed the documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required. The ST and AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that section 4 of AGD identifies each resource required by the TOE. These resources include, • Network Connectivity • Camera • Microphone • Location Services This list of resources is consistent with the resources identified in the ST. Next, the evaluator verified that for each resource, section 4 of AGD provides a justification of why access to the resource is required. Based on these finds, this activity is considered satisfied.
Verdict	Pass

6.1.26 *FDP_DEC_EXT.1.1 Test 1*

Table 29 – FDP_DEC_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_DEC_EXT_1_1_T1
Objective	The evaluator shall verify that either the application or the documentation provides a list of the hardware resources it accesses.
Evaluator Findings	The evaluator verified that either the application or the documentation provides a list of the hardware resources it accesses. The TOE itself and AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that section 4 of AGD provides a list of the hardware resources the TOE accesses. This includes, • Network Connectivity • Camera • Microphone • Location Services This list is consistent with the list presented in the ST. Additionally, the TOE itself provides an identification that Location, Camera, and Microphone are being accessed upon use. This was demonstrated via testing, as described below. Based on these findings, this activity is considered satisfied.
Test Flow	• Start “Safari” and visit “maps.google.com”. • “Safari” will prompt the user asking whether to allow or disallow “Safari” to access Location Services. • If the user allows the access to Location Services then it can also be viewed under “Settings”-> “Privacy”-> “Location Services”->”Safari Websites”. • Safari also provides the user an option to enable “Camera and Microphone Access”. This can be viewed under “Settings”-> “Safari”->”Camera and Microphone Access”.

Pass/Fail Explanation	Safari provides the user with a list of required hardware resources. This meetings the testing requirements.
Result	Pass

6.1.27 *FDP_DEC_EXT.1.1 Guidance 1*

Table 30 – FDP_DEC_EXT.1.2 Guidance	
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. For iOS: The evaluator shall verify that either the application software or its documentation provides a list of the sensitive information repositories it accesses.	
Evaluator Findings	The evaluator reviewed the documentation provided by the application developer and for each sensitive information repository which it accesses, identified the justification as to why access is required. The TOE itself, ST, and AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE does not access sensitive information repositories. This is consistent with the documentation. Based on these findings, this activity is considered satisfied.
Result	Pass

6.1.28 *FDP_NET_EXT.1.1 Test 1*

Table 31 – FDP_NET_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_NET_EXT.1.1_T1
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
Pass/Fail Explanation	The TOE only sends user initiated TLS traffic as expected. This meets the testing requirements.
Result	Pass

6.1.29 *FDP_NET_EXT.1.1 Test 2*

Table 32 – FDP_NET_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_NET_EXT.1.1_T2
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	• Execute nmap -Pn <IP-Address> prior to exercising the application • Initialize and engage with the application to perform some activity.

	• Execute nmap -Pn <IP-Address> after exercising the application
Pass/Fail Explanation	The TOE did not open any unexpected ports. This meets the testing requirements.
Result	Pass

6.1.30 *FDP_ACF_EXT.1.1 TSS*

Table 33 – FDP_ACF_EXT.1.1 TSS	
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 to ensure it describes how the browser separates local and session storage. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that The TOE runs in a sandbox environment within the underlying platform OS. The TOE has not access to storage outside of the implemented sandbox. The storage used by the TOE is isolated from the underlying platform. Based on these findings, this activity is considered satisfied.
Result	Pass

6.1.31 *FDP_ACF_EXT.1.1 Guidance*

Table 34 – FDP_ACF_EXT.1.1 Guidance	
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.
Result	Pass

6.1.32 *FDP_ACF_EXT.1.1 Test 1*

Table 35 – FDP_ACF_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_ACF_EXT.1.1_T1
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: Test 1: The evaluator shall open two or more browser windows/tabs and navigate to the same web page. The evaluator shall verify that the script for accessing session storage that is running in 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 https://blog.guya.net/security/browser_session/sessionStorage.html that allows the user to set session storage.
	  ○ 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.

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

6.1.33 *FDP_ACF_EXT.1.1 Test 2*

Table 36 – FDP_ACF_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_ACF_EXT.1.1_T2
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: Test 2: 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.
Note	This test is performed in conjunction with FDP_SOP_EXT.1.1 Test#1. The TOE implements Same Origin Policy (SOP).
Pass/Fail Explanation	The evaluator observed that the script running in one window did not access information associated with a different window. This meets the testing requirements.
Result	Pass

6.1.34 *FDP_COO_EXT.1.1 TSS*

Table 37 – FDP_COO_EXT.1.1 TSS	
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 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). The TSS of the ST was used to determine the verdict of this activity. 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 activity is considered satisfied.
Result	Pass

6.1.35 *FDP_COO_EXT.1.1 Guidance*

Table 38 – FDP_COO_EXT.1.1 Guidance	
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 and Other Tracking Behavior & Security Features" of 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

6.1.36 *FDP_COO_EXT.1.1 Test 1*

Table 39 – FDP_COO_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_COO_EXT.1.1_T1
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: Test 1: 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 iOS Device (iPhone/iPad): ○ Within iPhone navigate to "Settings" ○ Navigate from "Settings" to "Safari" ○ Within "Safari", click on "Clear History and Data". Click "Clear" ○ Within "Safari" navigate to "Advanced" and Enable "Web Inspector" ○ Connect the iOS device to Macbook with a USB cable ○ Start "Safari" browser ○ Open https://www.linkedin.com • 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”.
Pass/Fail Explanation	The evaluator loaded a web page and verified that the cookie was stored. This meets the testing requirements.
Result	Pass

6.1.37 *FDP_COO_EXT.1.1 Test 2*

Table 40 – FDP_COO_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_COO_EXT.1.1_T1
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: Test 2: 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 iPhone navigate to “Settings” ○ Navigate from “Settings” to “Safari” ○ Within “Safari” click on “Block All Cookies” ○ Within “Safari” navigate to “Advanced” and Enable “Web Inspector” • 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 no Cookies are stored as we have blocked all cookies.
Pass/Fail Explanation	The evaluator loaded a web page and verified that the cookie was not stored. This meets the testing requirements.
Result	Pass

6.1.38 *FDP_SBX_EXT.1.1 TSS*

Table 41 – FDP_SBX_EXT.1.1 TSS
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 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). The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that 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 evaluator checked 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. Upon investigation, the evaluator found that the TOE runs in a dedicated sandbox environment on the platform. This completely isolates the requests from accessing the platform's file system. Finally, the evaluator confirmed that the TSS states that this functionality is enabled automatically with no required user intervention. Based on these findings, this activity is considered satisfied.
Result	Pass

6.1.39 *FDP_SBX_EXT.1.1 Guidance*

Table 42 – FDP_SBX_EXT.1.1 Guidance	
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 5.2, "Sandboxing of Rendering Processes," of 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.
Result	Pass

6.1.40 *FDP_SBX_EXT.1.1 Test 1*

Table 43 – FDP_SBX_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_SBX_EXT.1.1_T1
Objective	The evaluator shall perform the following test on each platform claimed in the ST: Test 1: 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.
Pass/Fail Explanation	No API currently exists that would allow the programmer to access the filesystem of an iOS device through Safari. Any APIs that do exist that would support this functionality are either not supported, or only allow read-only access to the server side scripts. Apple Documentation that displays all supported APIs for Safari (note the absence of any file access APIs that allow write access) - https://developer.apple.com/documentation/webkitjs All available APIs - https://developer.mozilla.org/en-US/docs/Web/API File API (all methods are read-only) - https://developer.mozilla.org/en-US/docs/Web/API/File FileSystem API (not supported by iOS) - https://developer.mozilla.org/en-US/docs/Web/API/FileSystem
Result	Pass

6.1.41 *FDP_SOP_EXT.1.1 TSS*

Table 44 – FDP_SOP_EXT.1.1 TSS	
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 of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that each Browser tab/window is individually isolated from the other open tabs and does not allow data to flow between or exceptions made due to state, condition, or origin of another tab. No sharing occurs between tabs/windows. The TOE is fully compliant with RFC 6454 in that the policy is applied to all web browser tab/windows independently. Additionally, the evaluator found that there is no relaxation of these restrictions. Based on these findings, this activity is considered satisfied.
Result	Pass

6.1.42 *FDP_SOP_EXT.1.1 Test 1*

Table 45 – FDP_SOP_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_SOP_EXT.1.1_T1
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: Test 1: 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	• Steps to follow on host machine ○ Start Burpsuite on host machine. Navigate to "Proxy" tab and click on "Options". ○ In "Proxy Listeners" click on loopback address (127.0.0.1:8080) and click "Edit". Change this address to the IP address of the host machine, and port number to 8086. ○ In "Proxy Listeners" check box next to "Running". ○ In "Proxy Listeners" click on "Import/Export CA Certificate" ○ In "Export" click on "Certificate in DER format". Save the certificate with .cer extension. • Steps to follow on iPhone ○ To install this certificate, Email the above certificate to yourselves. On iPhone, Open the email in Safari browser. Click on the certificate. ○ Safari browser will ask the user for permission to install this certificate on iPhone. Click "Allow". ○ iPhone will prompt the user to install the profile, Click on "Install". Enter your passcode. Click "Install". ○ On iPhone, navigate to "Settings". Click on "Wifi" (if connected to an existing wifi connection). Click on "i" symbol next to wifi connection. Scroll to bottom. ○ Click on "Configure Proxy" and enter the host machine IP and port number. Click on "Save". ○ Verify that you can see the traffic in Burpsuite. ○ Start Safari instance and visit "https://greebo.net/2009/06/09/httponly-in-safari-40-release/" • Click on Test Script (see below screenshot)
Pass/Fail Explanation	Safari has implemented Same-Origin Policy. This meets the testing requirements
Result	Pass

6.1.43 *FDP_SOP_EXT.1.1 Test 2*

Table 46 – FDP_SOP_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_SOP_EXT.1.1_T2
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: Test 2: The evaluator shall verify that the scripts can retrieve content from another window/tab at a different subdomain
Note	The above test FDP_SOP_EXT.1 Test #1 shows that the TOE implements Same Origin Policy (SOP). The TOE does not implement a relaxation of these rules for subdomains.
Result	Pass

6.1.44 *FDP_STR_EXT.1.1 TSS*

Table 47 – FDP_STR_EXT.1.1 TSS	
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 of 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.
Result	Pass

6.1.45 *FDP_STR_EXT.1.1 Test 1*

Table 48 – FDP_STR_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_STR_EXT.1.1_T1
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: Test 1: 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	• *Steps to follow on iOS device (iPhone/iPad)*
	  ○ Navigate to iOS Settings.
	  ○ Click on Safari
	  ○ Click on Advanced

	○ Enable Web Inspector ○ Initialize Safari. ○ Visit: https://ec2-34-212-23-85.us-west-2.compute.amazonaws.com:9999/ • *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 that the cookies are set with Secure Flag.*
Pass/Fail Explanation	The website https://ec2-34-212-23-85.us-west-2.compute.amazonaws.com:9999/ presented a Secure cookie to the TOE. This meets testing requirements.
Result	Pass

6.1.46 *FDP_STR_EXT.1.1 Test 2*

Table 49 – FDP_STR_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_STR_EXT.1.1_T2
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: Test 2: The evaluator shall reconnect to the cookie-enabled website over an insecure channel and verify that no "secure" cookie is sent.
Test Flow	• *Steps to follow on iOS device* ○ Navigate to iOS Settings. ○ Click on Safari ○ Click on Advanced ○ Enable Web Inspector ○ Initialize Safari. ○ Visit: http://ec2-34-212-23-85.us-west-2.compute.amazonaws.com:9999/ • *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 that the cookies are not set with Secure Flag.*
Pass/Fail Explanation	The website did not send Secure cookie to the TOE. This meets the testing requirements.
Result	Pass

6.1.47 *FDP_TRK_EXT.1.1 TSS*

Table 50 – FDP_TRK_EXT.1.1 TSS	
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 of 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.
Result	Pass

6.1.48 *FDP_TRK_EXT.1.1 Guidance*

Table 51 – FDP_TRK_EXT.1.1 Guidance	
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 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.
Result	Pass

6.1.49 *FDP_TRK_EXT.1.1 Test 1*

Table 52 – FDP_TRK_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FDP_TRK_EXT.1.1_T1
Objective	The evaluator shall perform the following tests for each type of tracking information listed in the TSS: Test 1: 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	• Steps to follow on iOS device (iPhone/iPad) • *Go to Settings, then General and click on Reset.* • *Click on "Reset Location and Privacy"* • *Start Safari. Open a Window/Tab and Visit https://maps.google.com* • *Click on "your location" available at the bottom right of the Application screen.* • *Accept the Geolocation and current location prompt.*
Pass/Fail Explanation	Safari notifies the user about tracking requests and upon consent retrieves tracking information. This meets the testing requirements.
Result	Pass

6.1.50 *FDP_TRK_EXT.1.1 Test 2*

Table 53 – FDP_TRK_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FDP_TRK_EXT.1.1_T2
Objective	The evaluator shall perform the following tests for each type of tracking information listed in the TSS: Test 2: 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	• Steps to follow on iOS device (iPhone/iPad) • *Go to Settings, then General and click on Reset.* • *Click on "Reset Location and Privacy"* • *Start Safari. Open a Window/Tab and Visit https://maps.google.com* • *Click on "your location" available at the bottom right of the Application screen.* • *Deny the Geolocation and current location prompt.*
Pass/Fail Explanation	Safari notifies the user about tracking requests and upon denial does not retrieve tracking information. This meets the testing requirements.
Result	Pass

6.1.51 *FDP_DAR_EXT.1.1 TSS*

Table 54 – FDP_DAR_EXT.1.1 TSS 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. 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.

Evaluator Findings	The evaluator inspected 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. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that 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 C (Protected Until First User Authentication - NSFileProtectionComplete). Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.52 *FIA_X509_EXT.1.1 TSS*

Table 55 – FIA_X509_EXT.1.1 TSS	
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 the TSS to determine that it describes where the check of validity of the certificates takes place. Section 6 of the ST was used to determine the verdict of this assurance activity. The evaluator found that certificate validation is performed by the TOE platform (iOS) in conformance to RFC5280. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.53 *FIA_X509_EXT.1.1 Test 1*

Table 56 – FIA_X509_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.1_T1
Objective	The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator shall then delete one of the certificates, and show that the function fails.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Attempt to connect to a peer using a certificate without a valid certification path • This results in an authenticate failure • Load the trusted CA certificate(s) needed to validate the peer's certificate • Demonstrate that the connection succeeds • Delete one of the CA certificates • Show that the connection fails
Pass/Fail Explanation	A connection is made when a full certificate chain is present. A connection is not made when a full certificate chain is not present. This meets the testing requirements.
Result	Pass

6.1.54 *FIA_X509_EXT.1.1 Test 2*

Table 57 – FIA_X509_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.1_T2
Objective	The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Change the time on the platform to a time in the future (when the server certificate is expired) • Attempt a connection with a sever using the certificate and verify the connection fails
Pass/Fail Explanation	The evaluator verified that validating an expired certificate resulted in function failing. This meets the testing requirements.
Result	Pass

6.1.55 *FIA_X509_EXT.1.1 Test 3*

Table 58 – FIA_X509_EXT.1.1 Test 3	
Item	**Data/Description**
Test ID	FIA_X509_EXT_1_1_T3
Objective	The evaluator shall test that the TOE can properly handle revoked certificates—conditional on whether CRL, OCSP, or OCSP Stapling is selected; if multiple methods are selected, then a test shall be performed for each method. • The evaluator shall test revocation of the node certificate • The evaluator shall also test revocation of and intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA), if intermediate CA certificates are supported. 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.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Make a connection • Ensure that a valid certificate is used, and that the validation function succeeds • Attempt the test with a certificate that has been revoked. • Ensure when the certificate is no longer valid that the validation function fails
Pass/Fail Explanation	A connection is possible when the presented certificate is not revoked. A connection is not made when the presented certificate is revoked. This meets the testing requirements.
Result	Pass

6.1.56 *FIA_X509_EXT.1.1 Test 4*

Table 59 – FIA_X509_EXT.1.1 Test 4

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T4
Objective	If OCSP 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.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Present a certificate that does not have the OCSP signing purpose • Verify that validation of the OCSP response fails
Pass/Fail Explanation	The connection is rejected when the OCSP response is signed using a certificate that does not have the OCSP signing purpose. This meets the testing requirements.
Result	Pass

6.1.57 *FIA_X509_EXT.1.1 Test 5*

Table 60 – FIA_X509_EXT.1.1 Test 5	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.1_T5
Objective	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.)
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Modify any byte in the first eight bytes of the certificate • Verify an attempt to connect to a server with that certificate fails
Pass/Fail Explanation	Connections attempts with servers presenting modified certificates fail. This meets the testing requirements.
Result	Pass

6.1.58 *FIA_X509_EXT.1.1 Test 6*

Table 61 – FIA_X509_EXT.1.1 Test 6	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.1_T6
Objective	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.)
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Modify any bit in the last byte of the certificate • Attempt to use the certificate and verify that the usage fails
Pass/Fail Explanation	It is not possible to use a certificate that has been modified. This meets the testing requirements.
Result	Pass

6.1.59 *FIA_X509_EXT.1.1 Test 7*

Table 62 – FIA_X509_EXT.1.1 Test 7	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.1_T7
Objective	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.)
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Modify any byte in the public key of the certificate • Demonstrate that the certificate fails to validate
Pass/Fail Explanation	It is not possible to use a certificate that has been modified. This meets the testing requirements.
Result	Pass

6.1.60 *FIA_X509_EXT.1.2 Test 1*

Table 63 – FIA_X509_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.2_T1
Objective	The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a certificate that does not contain the basicConstraints extension • Verify that certificate validation fails.
Pass/Fail Explanation	Incomplete certificates (without the basicConstraints extension) fail to validate and are rejected. This meets the testing requirements.
Result	Pass

6.1.61 *FIA_X509_EXT.1.2 Test 2*

Table 64 – FIA_X509_EXT.1.2 Test 2	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.2_T2
Objective	The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the CA flag in the basicConstraints extension not set. The validation of the certificate path fails.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Test Flow	• Create a certificate of the CA issuing the TOE's certificate has the CA flag in the basicConstraints extension not set • Verify that certificate validation fails.
Pass/Fail Explanation	Certificates without the basicConstraints extension set fail to validate and are rejected. This meets the testing requirements.

Result	Pass

6.1.62 *FIA_X509_EXT.1.2 Test 3*

Table 65 – FIA_X509_EXT.1.2 Test 3	
Item	**Data/Description**
Test ID	FIA_X509_EXT.1.2_T3
Objective	The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the CA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Pass/Fail Explanation	This test was performed in conjunction with FCS_TLSC tests where a connection was successfully established. Those tests demonstrated the ability to verify a CA when basicConstraints is set to TRUE.
Result	Pass

6.1.63 *FIA_X509_EXT.2.2 TSS*

Table 66 – FIA_X509_EXT.2.2 TSS	
The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. 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. 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 checked the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the certificate used for TLS connection are loaded as all other configuration information is loaded, via an .xml configuration file. The TOE will only use the configured certificates for TLS connections. Next, the evaluator examined 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. Upon investigation, the evaluator found that if during the revocation check of the certificate, the OCSP server cannot be contacted, the connection will not be established. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.64 *FIA_X509_EXT.2.2 Test 1*

Table 67 – FIA_X509_EXT.2.2 Test 1

Item	Data/Description
Test ID	FIA_X509_EXT.2.2_T1
Objective	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.
Note	This test case leverages the testing which has previously been vetted and approved as part of VID 10937. This approach has been vetted by the NIAP/NIAP validators.
Pass/Fail Explanation	This test was covered by X509_EXT.1.1_TEST 3.
Result	Pass

6.1.65 *FMT_MEC_EXT.1.1 TSS 1*

Table 68 – FMT_MEC_EXT.1.1 TSS	
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. 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 reviewed 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. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE supports the following configurations, • 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 auto-fill 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 Next, the evaluator identified that each of these settings are stored in the user defaults system by the underlying platform. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.66 *FMT_MEC_EXT.1.1 Test 1*

Table 69 – FMT_MEC_EXT.1.1 Test 1

Item	Data/Description
Test ID	FMT_MEC_EXT_1_1_T1
Objective	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.Safari.SafeBrowsing.BrowsingDatabases.Update • Execute command: defaults read com.apple.SafariBookmarksSyncAgent.XPC.ZoneSubscriptionRegistration • Execute command: defaults read com.apple.safariBookmarksSyncAgent.migration • Execute command: defaults read com.apple.accessoryd.plugin
Pass/Fail Explanation	The TOE uses user defaults system for storing all settings.
Result	Pass

6.1.67 *FMT_CFG_EXT.1.1 TSS 1*

Table 70 – FMT_CFG_EXT.1.1 TSS	
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 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

6.1.68 *FMT_CFG_EXT.1.1 Test 1*

Table 71 – FMT_CFG_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FMT_CFG_EXT_1_1_T1
Objective	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 per the test case, this test case is not applicable, “If the application uses any default credentials the evaluator shall run the following tests.”
Result	Not Applicable

6.1.69 *FMT_CFG_EXT.1.1 Test 2*

Table 72 – FMT_CFG_EXT.1.1 Test 2	
Item	**Data/Description**

Test ID	FMT_CFG_EXT_1_1_T2
Objective	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 per the test case, this test case is not applicable, "If the application uses any default credentials the evaluator shall run the following tests."
Result	Not Applicable

6.1.70 *FMT_CFG_EXT.1.1 Test 3*

Table 73 – FMT_CFG_EXT.1.1 Test 3	
Item	**Data/Description**
Test ID	FMT_CFG_EXT_1_1_T3
Objective	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 per the test case, this test case is not applicable, "If the application uses any default credentials the evaluator shall run the following tests."
Result	Not Applicable

6.1.71 *FMT_CFG_EXT.1.2 Test 1*

Table 74 – FMT_CFG_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FMT_CFG_EXT_1_2_T1
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.
Note	The application does not create any files that are available in the user accessible files system. Apple iOS does not allow for direct access to system files such as Safari.
Test Flow	• Review Apple iOS 12 Security Guide (attached in Execution Output) • In iOS Security Guide, search for "Keychain Data Protection" • In iOS Security Guide, search for "Data Protection Classes" • In iOS Security Guide, search for Search for "Data Protection Class key"
Pass/Fail Explanation	iOS Safari uses "kSecAttrAccessibleWhenUnlocked" Keychain Data Protection. iOS Safari implements Data Protection class A or Complete Protection. This meets the testing requirement.
Result	Pass

6.1.72 *FMT_MOF_EXT.1.1 TSS*

Table 75 – FMT_MOF.1.1 TSS

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 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 ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that enabling and disabling JavaScript and enabling and disabling storage of auto-fill and auto-complete data can be configured via uploaded profiles. When configured via an uploaded profile, the user of the TOE is not able to change the settings. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.73 *FMT_MOF_EXT.1.1 Guidance*

Table 76 – FMT_MOF.1.1 Guidance	
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 and Other Tracking Behavior & Security Features," within AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found the following administrative activities described, • Enable/disable storage of third party cookies • Prevent websites from tracking you • Prevent cross-site tracking • Clear 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. • Clear AutoFill information • Clear cookies and keep history • Configure malicious application/URL detection • Enable/disable 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

6.1.74 *FMT_MOF_EXT.1.1 Test 1*

Table 77 – FMT_MOF_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FMT_MOF_EXT_1_1_T1
Objective	The evaluator shall verify that functions perform as intended by enabling, disabling, and configuring the functions

Test Flow	• Go to Settings -> Safari -> Enable Javascript and Click on Website data. • Start Safari and visit 1. https://www.niap-ccevs.org and 2. https://www.apple.com • Go to Settings -> Safari -> Click on Website Data and Click on Remove All Website Data. • Go to Settings -> Safari -> Privacy & Security. • Enable/Disable ->Prevent Cross-Site Tracking, Block All Cookies, Ask Websites Not To Track Me, Fraudulent Website Warning. • Click on General -> Click on Autofill and Enable/Disable 1. Use Contact Info and 2. Credit Cards.
Pass/Fail Explanation	The tester verified that Safari Management functions can be enabled, disabled and configured as intended. This meets the testing requirements.
Result	Pass

6.1.75 *FMT_MOF_EXT.1.1 Test 2*

Table 78 – FMT_MOF_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FMT_MOF_EXT_1_1_T2
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
Test Flow	• *Start Apple Configurator* • *Create a new profile with the restrictions* • *Install this profile on the iOS device.* • *Attempt to override these restrictions/policies as a user.* ○ *The restrictions that cannot be overridden are Greyed out.* • *Verify that the TOE does not permit the overriding.*
Pass/Fail Explanation	The evaluator attempted to override policies as an user and verified that the user was not able to override any policies. This meets the testing requirements.
Result	Pass

6.1.76 *FMT_SMF.1.1 Guidance*

Table 79 – FMT_SMF.1.1 Guidance	
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 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,

	• Enable/disable storage of third party cookies • Prevent websites from tracking you • Prevent cross-site tracking • Clear 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. • Clear AutoFill information • Clear cookies and keep history • Configure malicious application/URL detection • Enable/disable JavaScript The evaluator found these management activities to be all inclusive of the management activities required by the PP. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.77 *FPR_ANO_EXT.1 TSS*

Table 80 – FPR_ANO_EXT.1.1 TSS	
The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.	
Evaluator Findings	The evaluator inspected the TSS documentation to identify functionality in the application where PII can be transmitted. The TSS of the ST was used to determine the verdict of this activity. 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 these findings, this activity is considered satisfied.
Verdict	Pass

6.1.78 *FPR_ANO_EXT.1 Test #1*

Table 81 – FPR_ANO_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FPR_ANO_EXT.1.1_T1
Objective	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	As stated, Safari does not expressly request any PII. Therefore, this test is considered satisfied.
Result	Pass

6.1.79 *FPT_DNL_EXT.1.1 TSS 1*

Table 82 – FPT_DNL_EXT.1.1 TSS	
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 examined the TSS to ensure that it describes the behavior of the browser when a user initiates the download of a file. The TSS of 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

6.1.80 *FPT_DNL_EXT.1.1 Guidance*

Table 83 – FPT_DNL_EXT.1.1 Guidance	
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 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

6.1.81 *FPT_DNL_EXT.1.1 Test 1*

Table 84 – FPT_DNL_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FPT_DNL_EXT.1.1_T1
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.
Note	*The evaluator hosted a custom Acumen Security Test tool at http://10.1.1.55., along with four different types of files for download 1. MS Windows Executable (.exe), 2. Security Certificate (.cer), 3. Debian package (.deb) and 4. iOS Package (.ipa).*

Test Flow	• Start Safari Browser.
	• Open http://10.1.1.55/test_tools/downloadcheck/downloadfiles.html in Safari.
	  ○ Click on "Download Sample Executable" (MS Windows Application)
	  ▪ Click on the arrow (pointing upwards) at the bottom of the new window.
	  ▪ Click on "Save to Files"
	  ▪ Verify that the file can be saved on "On my iPhone" (in case of iPad- "On my iPad")

	▪ Navigate to “Files” application on iPhone. Attempt to open the downloaded file. o Click on “Download Sample Security Certificate” ▪ Safari will show a pop-up to the User. ▪ Click on “Allow” ▪ iOS will prompt the User to Install the Profile. ▪ Click on “Install”. Enter “Passcode”. Click Done. ▪ Click on “Install”. Click on “Done”. Click on “PortSwigger CA”. ▪ Click on “More Details”. Click on “PortSwigger CA” Scroll until bottom. o Click on “Download Sample DEB File” (Debian Package) ▪ Click on the arrow (pointing upwards) at the bottom of the new window. ▪ Click on “Save to Files” ▪ Verify that the file can be saved on “On my iPhone” (in case of iPad- “On my iPad”) ▪ Navigate to “Files” application on iPhone. Attempt to open the downloaded file. o Click on “Download Sample IPA File#1” (iOS Package) ▪ Click on the arrow (pointing upwards) at the bottom of the new window. ▪ Click on “Save to Files” ▪ Verify that the file can be saved on “On my iPhone” (in case of iPad- “On my iPad”) ▪ Navigate to “Files” application on iPhone. Attempt to open the downloaded file. • Exit Safari Browser.
Pass/Fail Explanation	Safari does not have the feature to present the user with a “dialog box” that could allow the user to download/delete a file, however, it does so by not providing “dialog box”. This meets the testing requirements.
Result	Pass

6.1.82 *FPT_MCD_EXT.1.1 TSS*

Table 85 – FPT_MCD_EXT.1.1 TSS	
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 to ensure it lists the types of signed mobile code that the browser supports. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE only supports JavaScript mobile code. Next, the evaluator verified that the TSS describes how the browser handles unsigned mobile code, mobile code from an untrusted source, and mobile code

	from an unverified source. Upon investigation, the evaluator found that all incorrectly signed JavaScript is discarded by the TOE. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.83 *FPT_MCD_EXT.1.1 Guidance*

Table 86 – FPT_MCD_EXT.1.1 Guidance	
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 describe 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.	
Evaluator Findings	The evaluator examined the operational guidance to verify it provides configuration instructions for each of the supported mobile code types. Section 6.2, "Mobile Code," of AGD in support of this activity. Upon investigation, the evaluator found that if the browser is presented unsigned, untrusted, or unverified JavaScript, the code is discarded and not executed. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.84 *FPT_MCD_EXT.1.1 Test 1*

Table 87 – FPT_MCD_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FPT_MCD_EXT.1.1_T1
Objective	The evaluator shall construct web pages containing unsigned, correctly authenticated, and incorrectly authenticated mobile code and ensure that the browser alerts the user when it encounters mobile code that fails to authenticate and provides the user with the option to discard the mobile code without executing it, but does execute signed mobile code that properly authenticates.
Test Flow	• Steps to follow on iPhone/iPad ○ Enable Web Inspector. ○ Click on Settings, scroll down until Safari. Click on Safari. ○ Scroll down to Advanced. Click on Advanced. Enable Web Inspector. ○ Connect iPhone/iPad to Macbook via USB. ○ Start Safari on Macbook and Enable Develop Menu. ○ Click on Safari, then Preferences, and then Advanced. Check "Show Develop menu in menu bar" ○ Start Safari on iPhone/iPad ▪ Establish a connection to https://scripts.acumensecurity.net/integritycheck.html (signed) ▪ Click on "Click for Valid JS". ▪ The Valid JS will execute as this file has correct hash. ○ Start Safari on iPhone/iPad

	▪ Establish a connection to https://scripts.acumensecurity.net/integritycheck.html (unsigned) ▪ Click on "Click for Invalid JS". ▪ Ensure the error is visible through Web Inspector. ▪ The invalid JS will not execute as this file has incorrect hash. ○ Start Safari on iPhone/iPad ▪ *Establish a connection to* https://scripts.acumensecurity.net:81/ (untrusted) ▪ *Safari will prevent the user from visiting the page because Safari attempts to leverage incorrect certificate (accomplished by adding random characters to the .key file and .crt file)* ○ Start Safari on iPhone/iPad ▪ *Establish a connection to* https://scripts.acumensecurity.net:7655/ (unverified) • *Safari will prevent the user from visiting the page because Safari attempts to connect with URL that has a self-signed certificate, meaning that that it does not connect to a CA.*
Pass/Fail Explanation	Safari executes signed mobile code but prevents execution of unsigned, untrusted or unverified mobile code. This meets the testing requirements.
Result	Pass

6.1.85 *FPT_AON_EXT.1.1 TSS 1*

Table 88 – FPT_AON_EXT.1.1 TSS	
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 of the ST was used to determine the verdict of the activity. Upon investigation, the evaluator found that the TOE does not support the capability of loading add-ons. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.86 *FPT_AON_EXT.1.1 Guidance*

Table 89 – FPT_AON_EXT.1.1 Guidance	
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 6.3, "Support for Add-ons," of 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

6.1.87 *FPT_AON_EXT.1.1 Test 1*

Table 90 – FPT_AON_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FPT_AON_EXT.1.1_T1
Objective	Test 1: 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 requirements is met implicitly.
Result	Pass

6.1.88 *FPT_AON_EXT.1.1 Test 2*

Table 91 – FPT_AON_EXT.1.1 Test 2	
Item	**Data/Description**
Test ID	FPT_AON_EXT.1.1_T2
Objective	Test 2: 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 requirements is met implicitly.
Result	Pass

6.1.89 *FPT_API_EXT.1.1 TSS*

Table 92 – FPT_API_EXT.1.1 TSS	
The evaluator shall verify that the TSS lists the platform APIs used in the application. 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.	
Evaluator Findings	The evaluator examined the TSS to determine if the platform APIs used in the application are listed. Section 6 of the ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE leverages the following API: • Accounts.framework • AppSupport.framework • AssistantServices.framework • CFNetwork.framework • Contacts.framework • ContactsUI.framework • CoreFoundation.framework • CoreGraphics.framework • CoreTelephony.framework • CoreText.framework • DataMigration.framework • DiagnosticExtensions.framework • Foundation.framework

	• GraphicsServices.framework • ImageIO.framework • IOKit.framework • JavaScriptCore.framework • LocalAuthentication.framework • ManagedConfiguration.framework • MapKit.framework • MobileCoreServices.framework • PlugInKit.framework • Preferences.framework • QuartzCore.framework • SafariSafeBrowsing.framework • SafariServices.framework • Security.framework • TelephonyUtilities.framework • UIKit.framework • WebBookmarks.framework • WebContentAnalysis.framework • WebKit.framework Next, the evaluator compared the API leveraged by the application to the available system resources. This included direct discussion with OS platform development teams, as well as, developer publications. Each of the listed API are applicable system API. Based on this the assurance activity is considered satisfied.
Verdict	Pass

6.1.90 *FPT_AEX_EXT.1.1 TSS*

Table 93 – FPT_AEX_EXT.1.1 TSS	
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 to determine if it describes the compiler flags used to enable ASLR. The TSS of 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

6.1.91 *FPT_AEX_EXT.1.1 Test 1*

Table 94 – FPT_AEX_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FPT_AEX_EXT_1_1_T1
Objective	The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled. 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 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	• Initialize the TOE. • ssh into the device. • Execute command: kill -s ABRT <PID> • Repeat the above two steps, thrice. • Save the logs. • Verify that the TOE does not remake any mmap calls and no arguments are provided that request a mapping at a fixed address
Pass/Fail Explanation	The TOE uses ASLR and does not include any explicit memory mapping. This meets the testing requirement.
Result	Pass

6.1.92 *FPT_AEX_EXT.1.2 Test 1*

Table 95 – FPT_AEX_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FPT_AEX_EXT_1_2_T1
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	• Initialize the TOE. • ssh into the device. • Execute command: kill -s ABRT <PID> • Verify that mprotect is never invoked with the PROT_EXEC permission.
Pass/Fail Explanation	The TOE uses ASLR and does not include any explicit memory mapping. This meets the testing requirement.
Result	Pass

6.1.93 *FPT_AEX_EXT.1.3 Test 1*

Table 96 – FPT_AEX_EXT.1.3 Test 1	
Item	**Data/Description**
Test ID	FPT_AEX_EXT_1_3_T1
Objective	The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests: For iOS: The evaluator shall ensure that the application can successfully run on the latest version of iOS.
Test Flow	• Go to Settings -> General -> About -> iOS Version • Start Safari and visit 1. https://www.niap-ccevs.org and 2. https://www.apple.com • Verify that Safari can load the above two websites.

Pass/Fail Explanation	Safari is shipped with iOS and hence the software version for Safari will be the same as that of iOS version. The tester observed that Safari was able to successfully run on the certified version of the TOE platform. This meets the test requirements.
Result	Pass

6.1.94 *FPT_AEX_EXT.1.4 Test 1*

Table 97 – FPT_AEX_EXT.1.4 Test 1	
Item	**Data/Description**
Test ID	FPT_AEX_EXT_1_4_T1
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

6.1.95 *FPT_AEX_EXT.1.5 TSS*

Table 98 – FPT_AEX_EXT.1.5 TSS	
The evaluator shall ensure that the TSS section of the ST describes the compiler flag used to enable stack-based buffer overflow protection in the application.	
Evaluator Findings	The evaluator examined the TSS to determine if it describes the compiled flag used to enable stack-based buffer overflow protection. The TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states that the TOE is compiled with the –fstack-protector-all flag in support of stack-based buffer overflow protection. Based on this, the assurance activity is considered satisfied.
Verdict	Pass

6.1.96 *FPT_AEX_EXT.1.5 Test 1*

Table 99 – FPT_AEX_EXT.1.5 Test 1	
Item	**Data/Description**
Test ID	FPT_AEX_EXT_1_5_T1
Objective	The evaluator shall perform a static analysis to verify that stack-based buffer overflow protection is present. The method of doing so varies per platform: For iOS: If the application is compiled using GCC or Xcode, the evaluator shall ensure that the - fstack- protector- strong or - fstack- protector- all flags are used. The - fstack- protector- all flag is preferred but - fstack- protector- strong is acceptable. If the application is built using any other compiler, then the evaluator shall determine that appropriate stack-protection has been used during the build process.
Test Flow	• Cd into Applications/MobileSafari.app

	• Run the Tool to verify that –fstack –protector –all is used • Execute command: otool -lv MobileSafari | grep stack • Verify that fstack-protector-all is used.
Pass/Fail Explanation	The TOE is compiled with –fstack –protector –all, as required. This meets the testing requirements.
Result	Pass

6.1.97 *FPT_TUD_EXT.1.1 Test 1*

Table 100 – FPT_TUD_EXT.1 Test 1	
Item	**Data/Description**
Test ID	FPT_TUD_EXT.1_T1
Objective	The evaluator shall check for an update using procedures described in the 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	• Review the iOS Security Guide and verify what the description of Safari distribution (attached below)
	• Verify the current version and if there if there is a new version available
	  ○ Tap "Settings"
	  ○ Tap "General"
	• Tap "About" and verify version.

Pass/Fail Explanation	The TOE leverages the defined update mechanisms and does not issue an error. This testing requirement is considered satisfied.
Result	Pass

6.1.98 *FPT_TUD_EXT.1.2 Test 1*

Table 101 – FPT_TUD_EXT.1.2 Test 1	
Item	**Data/Description**
Test ID	FPT_TUD_EXT_1_2_T1
Objective	The evaluator shall verify that application updates are distributed in the format supported by the platform. This varies per platform: For iOS: The evaluator shall ensure that the application is packaged in the IPA format.
Test Flow	Review the iOS Security Guide and verify what the description of Safari distribution
Pass/Fail Explanation	iOS platform only supports IPA files.
Result	Pass

6.1.99 *FPT_TUD_EXT.1.3 Test 1*

Table 102 – FPT_TUD_EXT.1.3 Test 1	
Item	**Data/Description**
Test ID	FPT_TUD_EXT.1.3_T1

Objective	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	Per the testing for iOS, this requirement is implicitly met.
Result	Pass

6.1.100 *FPT_TUD_EXT.1.4 Test 1*

Table 103 – FPT_TUD_EXT.1.4 Test 1	
Item	**Data/Description**
Test ID	FPT_TUD_EXT.1.4_T1
Objective	The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the TSS. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.
Test Flow	• *Copy Safari Application directory from iOS device to MacBook before initialization and generate hash for each file in Safari Application directory.* • *Initialize and exercise Safari application.* • *Copy Safari Application directory from iOS device to MacBook after initialization and generate hash for each file in Safari Application directory.* • *Execute the custom script "shasumfiles.sh" and verify that the hashes match* • *Execute command: "diff Before-MobileSafari.txt* After-MobileSafari.txt*"* • *The evaluator confirmed that there were no differences in the above files*
Pass/Fail Explanation	The TOE does not modify any executable files. This meets the testing requirements.
Result	Pass

6.1.101 *FPT_TUD_EXT.1.5 Test 1*

Table 104 – FPT_TUD_EXT.1.5 Test 1	
Item	**Data/Description**
Test ID	FPT_TUD_EXT.1.5_T1
Objective	The evaluator shall query the application for the current version of the software according to the operational user guidance (AGD_OPE.1) and shall verify that the current version matches that of the documented and installed version
Note	*This test is performed in conjunction with FPT_TUD_EXT.1.1 Test#1*
Result	Pass

6.1.102 *FPT_TUD_EXT.1.6 TSS 1*

Table 105 – FPT_TUD_EXT.1.6 TSS

The evaluator shall verify that the TSS identifies how the application installation package and updates to it 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. iOS 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 the App Store and current versions of the TOE can be checked through the Settings 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

6.1.103 *FPT_LIB_EXT.1.1 Test 1*

Table 106 – FPT_LIB_EXT.1 Test 1	
Item	**Data/Description**
Test ID	FPT_LIB_EXT.1_T1
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 the command: ls -alR <application directory> (This will show everything installed) • Verify that no 3rd party libraries are installed
Pass/Fail Explanation	The TOE is installed with no 3rd party libraries. These meets the testing requirements.
Result	Pass

6.1.104 *FPT_DIT_EXT.1.1 TSS 1*

Table 107 – FPT_TUD_EXT.1.6 TSS	
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 examined the TSS to determine if it identifies the call to invoke platform provided functionality. Section 6 of the ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE invokes platform provided HTTPS/TLS using the NSURLSession class. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6.1.105 *FTP_DIT_EXT.1.1 Test 1*

Table 108 – FTP_DIT_EXT.1 Test 1	
Item	**Data/Description**
Test ID	FTP_DIT_EXT.1_T1
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 or DTLS in accordance with the selection in the ST
Note	*This test is performed in conjunction with FTP_DIT_EXT.1. Test#2*
Result	Pass

6.1.106 *FTP_DIT_EXT.1.1 Test 2*

Table 109 – FTP_DIT_EXT.1 Test 2	
Item	**Data/Description**
Test ID	FTP_DIT_EXT.1_T2
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://workbench.cisecurity.org • Establish a connection to https://ccusersforum.onlyoffice.com • Enter User credentials and Login to the both web applications
Pass/Fail Explanation	The TOE does not send any sensitive data in plaintext. This meets the testing requirements.
Result	Pass

6.1.107 *FTP_DIT_EXT.1.1 Test 3*

Table 110 – FTP_DIT_EXT.1 Test 3	
Item	**Data/Description**
Test ID	FTP_DIT_EXT.1_T3
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 credentials. Therefore, this is not applicable.
Result	Not Applicable

7 Security Assurance Requirements

7.1 ADV_FSP.1 Development

Table 111 – ADV_FSP.1 Development	
There are no specific assurance activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1, 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 assurance 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 1

Table 112 – AGD_OPE.1 Guidance 1	
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.	
Evaluator Findings	Section 3 of 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. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_OPE.1 Guidance 2

Table 113 – AGD_OPE.1 Guidance 2	
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 hash/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 2 of 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

7.4 AGD_PRE.1 Guidance

Table 114 – AGD_PRE.1 Guidance	
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 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 AGD identifies each of the platforms. Additionally, AGD provides a pointer to VID 10937. This is VID of the platform the TOE resides within. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.5 ALC_CMC.1 ST

Table 115 – ALC_CMC.1 ST	
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 12.3.1 Safari on iPhone and iPad. 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

7.6 ALC_CMS.1 Guidance

Table 116 – ALC_CMS.1 Guidance
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 assurance 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. FPT_AEX_EXT.1.5 listed in the ST identifies how buffer overflow protection is invoked. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.7 ALC_TSU_EXT.1 TSS 1

Table 117 – ALC_TSU_EXT.1 TSS 1	
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 10 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. Section 5.6 states of ST states Apple uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.8 ALC_TSU_EXT.1 TSS 2

Table 118 – ALC_TSU_EXT.1 TSS 2
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 evaluator also verified that this time is expressed in a number or range of days. The TSS and section 5.6 of the ST was used to determine the verdict of this assurance activity. After review, the evaluator found that the Apple "uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure". Based on these findings, the assurance activity is considered satisfied.
Verdict	Pass

7.9 ATE_IND.1 Test 1

Table 119 – ATE_IND.1 Test 1	
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 Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance 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 affect; 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 (IPsec, TLS, 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

7.10 AVA_VAN.1 Test 1

Table 120 – AVA_VAN.1 Test 1	
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 sources of the publicly available information are provided below. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • General web search (Google) • http://nvd.nist.gov/ • https://www.exploit-db.com/search • http://www.securityfocus.com • https://support.apple.com/en-us/HT209106 • https://support.apple.com/en-us/HT209192 The evaluator performed the public domain vulnerability searches using the following key words on January 25, 2019. • Apple iOS Safari • Webkit • Apple Framework The evaluator selected the search key words based upon the following criteria. • The product name was searched, • Key platform features the product leverages were searched The search returned applicable vulnerabilities, so the TOE was updated to version 12.1.4, which fixes the publicly known vulnerabilities. A follow-up vulnerability search was performed on March 1, 2019. Version 12.1.4 is the latest version of the TOE, and the vendor "reserves" all CVE descriptions until an update is available. For this reason, the updated vulnerability search focused on public web searches for potentially irresponsibly disclosed zero-day exploits.

	The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.
	• www.securityfocus.com
	• General web search (exploit, vulnerability, and zero day were appended to the search term) for:
	  ○ iOS 12.1.4
	  ○ Safari 12.1.4
	• https://www.exploit-db.com/search iOS vulnerabilities for:
	  ○ Webkit
	  ○ Safari
	The evaluator selected the search key words based upon the following criteria.
	• The product name was searched,
	• Key platform features the product leverages were searched
	• Focus on irresponsibly disclosed exploits
	The search returned no applicable vulnerabilities.
	A final vulnerability search was performed on June 4, 2019. Version 12.3.1 is the latest version of the TOE, and the vendor "reserves" all CVE descriptions until an update is available. For this reason, the updated vulnerability search focused on public web searches for potentially irresponsibly disclosed zero-day exploits.
	The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.
	• www.securityfocus.com recent Apple vulnerabilities
	• General web search (exploit, vulnerability, and zero day were appended to the search term) for:
	  ○ iOS 12.3.1
	  ○ Safari 12.3.1
	• https://www.exploit-db.com/search iOS vulnerabilities for:
	  ○ Webkit
	  ○ Safari
	The evaluator selected the search key words based upon the following criteria.
	• The product name was searched,
	• Key platform features the product leverages were searched
	• Focus on irresponsibly disclosed exploits
	The search returned no applicable vulnerabilities.

Verdict	Pass

7.11 AVA_VAN.1 Test 2

Table 121 – AVA_VAN.1 Test #2	
Item	Data/Description
Test ID	AVA_VAN.1_T2
Objective	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
Note	Virus Scanner Used: *McAfee Mobile Security v3.0.3*
Test Flow	• Scan the TOE with a virus scanner

	• Verify that the TOE was not flagged as a virus
Pass/Fail Explanation	When scanned by a virus scanner, the TOE is not identified as a virus.
Result	Pass

8 Conclusions

All testing and assurance activities pass.

---End of Document---