# Common Criteria SWAPP Assurance Activity Report Apple iOS 11 Contacts

Acumen Security

**ISSUED BY**

Acumen Security

Revision History:

| Version | Date | Changes |
|---|---|---|
| **Version 1.0** | June 2018 | Initial Release |
| **Version 1.1** | July 2018 | Updated based on internal review |
| **Version 1.2** | August 2018 | Updated based on ECR comments |
| **Version 1.3** | September 2018 | Updated based on ECR comments |
| **Version 1.4** | September 2018 | Updated based on review |

**Evaluation Technical Report for a Target of Evaluation**

**Apple IOS 11 Contacts on iPhone and iPad**

Security Target, version 0.4
Application Software Protection Profile, version 1.2

**Evaluated by:**


2400 Research Blvd Suite #340
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:**
Anthony Busciglio
Danielle F Canoles
Rutwij Kulkarni

**Common Criteria Version**
Common Criteria Version 3.1 Revision 4

**Common Evaluation Methodology Version**
CEM Version 3.1 Revision 4

Table of Contents

List of Tables

# 1 TOE Overview

The TOE is the Apple iOS 11 Contacts on iPhone and iPad. The product provides access and management of user contact information within the devices.

Note: The TOE is the application software only. The Apple iOS operating system has been separately validated (VID 10851).

## *1.1 TOE Description*

The TOE is an application on a mobile OS. The TOE is the Contacts application only. The Apple iOS operating system has been separately validated (VID 10851). The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 11.

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

**Table 1 – Evaluated Platforms**

| Device Name | Model | Processor | WiFi | Bluetooth |
|---|---|---|---|---|
| **iPhone X** | A1901<br>A1902<br>A1865 | A11 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 5.0 |
| **iPhone 8 Plus/ iPhone 8** | A1864, A1897, A1898, A1899/<br>A1863, A1905, A1906, A1907 | A11 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 5.0 |
| **iPhone 7 Plus/ iPhone 7** | A1661, A1784, A1785, A1786/<br>A1660, A1778, A1779, A1780 | A10 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPhone 6S Plus/ iPhone 6S** | A1634, A1687, A1690, A1699/<br>A1633, A1688, A1691, A1700 | A9 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPhone SE** | A1662<br>A1723<br>A1724 | A9 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2 |
| **iPhone 6 Plus/ iPhone 6** | A1522, A1524, A1593/<br>A1549, A1586, A1589 | A8 | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.0<br>4.0<br>4.0 |
| **iPhone 5s** | A1453<br>A1457<br>A1518<br>A1528<br>A1530<br>A1533 | A7 | 802.11a/b/g/n<br>802.11a/b/g/n<br>802.11a/b/g/n<br>802.11a/b/g/n<br>802.11a/b/g/n<br>802.11a/b/g/n | 4.0<br>4.0<br>4.0<br>4.0<br>4.0<br>4.0 |
| **iPad mini 3** | A1599<br>A1600<br>A1601 | A7 | 802.11a/b/g/n<br>802.11a/b/g/n<br>802.11a/b/g/n | 4.0<br>4.0<br>4.0 |
| **iPad mini 4** | A1538<br>A1550 | A8 | 802.11a/b/g/n<br>802.11a/b/g/n | 4.2<br>4.2 |
| **iPad Air 2** | A1566<br>A1567 | A8X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPad (5th gen)** | A1822<br>A1823 | A9X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPad Pro 12.9" (1st Gen)** | A1584<br>A1652 | A9X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPad Pro 9.7"** | A1673<br>A1674 | A9X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPad Pro 12.9" (2nd Gen)** | A1670<br>A1671 | A10X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |

| | | | | |
|---|---|---|---|---|
| **iPad Pro 10.5”** | A1701<br>A1709 | A10X | 802.11a/b/g/n/ac<br>802.11a/b/g/n/ac | 4.2<br>4.2 |
| **iPad 9.7”** | A1893<br>A1954 | A10 | 802.11a/b/g/n/ac | 4.2 |

The Operating System on which the TOE is running is Apple iOS version 11. 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 Assurance Activities Identification

The following table identifies each of the Assurance Activities (testing and documentation review) executed for this evaluation.

| Requirement | Auditable Event |
|---|---|
| FCS_HTTPS_EXT.1 | HTTPS Protocol |
| FCS_RBG_EXT.1 | Cryptographic Operation  Keyed Hash Message Authentication |
| FCS_STO_EXT.1 | Storage of Secrets |
| FCS_TLSC_EXT.1 | TLS Client Protocol |
| FCS_TLSC_EXT.4 | TLS Client Protocol |
| 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_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_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 11.

## *3.2 Processor Analysis*

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

- Apple A11
- Apple A10X
- Apple A10
- Apple A9X
- Apple A9
- Apple A8X
- Apple A8
- Apple A7

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 11. 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 A7, Apple A8, Apple A8X, Apple A9, Apple A9X, Apple A10, Apple A10X, and Apple A11. The following will be used for testing,

| Device | CPU Model | Operating System |
|---|---|---|
| **iPhone 5S** | A7 | Apple iOS11 |
| **iPhone 6 Plus** | A8 | Apple iOS11 |
| **iPad Air 2** | A8X | Apple iOS11 |
| **iPhone 6S Plus** | A9 | Apple iOS11 |

| | | |
|---|---|---|
| **iPad Pro 9.7** | A9X | Apple iOS11 |
| **iPhone 7** | A10 | Apple iOS11 |
| **iPad Pro** | A10X | Apple iOS11 |
| **iPhone 8 Plus** | A11 | Apple iOS11 |

# 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 (VID10851). 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 VID10851. 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: Note, FCS_TLSC_EXT.2.1 in the MD PP was used for this test case because they are equivalent
- 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

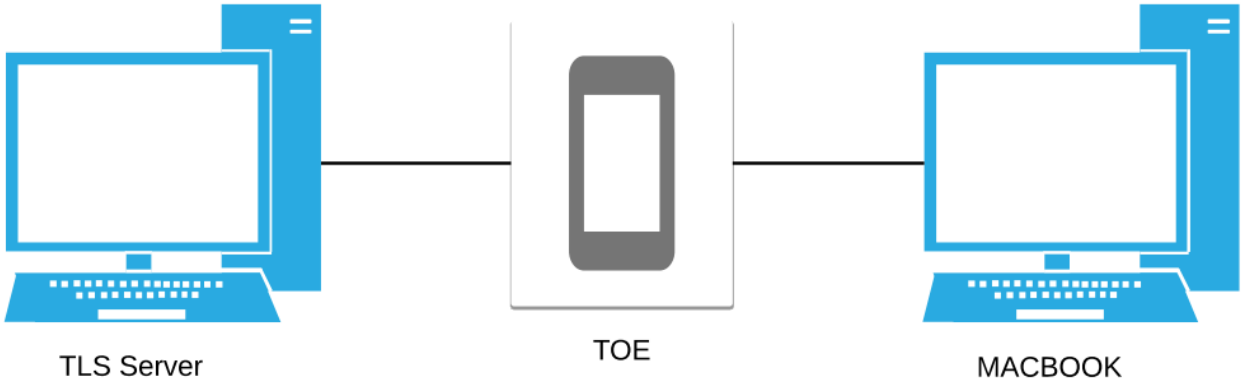
This is reflected in the note section of each of the applicable test cases.

# 5 Test Diagram

## *5.1 Application Specific Test Bed*

### 5.1.1 Visual Diagram

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




### 5.1.2 Configuration Information

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

#### 5.1.2.1 TOE

- OS: Apple iOS 11
- TOE: Apple iOS 11 Contacts

#### 5.1.2.2 TLS Server

- Application: OpenSSL

#### 5.1.2.3 Mac Book

- Application: OpenSSH

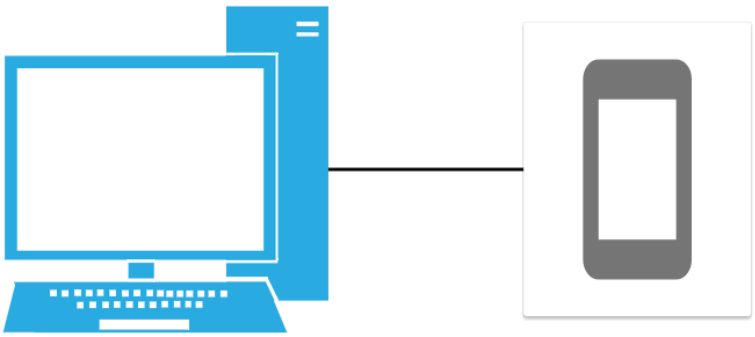
#### 5.1.2.4 Tooling

- nmap version 7.70
- Wireshark 2.6.1
- SSH version OpenSSH_7.6p1
- QuickTime Player (for Video Recording) version 10.4 [Platform: MAC]
- Custom Script - "shasumfiles.sh" for FPT_TUD_EXT.1.1 Test#1

## *5.2 Platform Test Bed*

### 5.2.1 Visual Diagram

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




### 5.2.2 Configuration Information

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

#### 5.2.2.1 TOE Platform

- OS: Apple iOS 11

#### 5.2.2.2 TLS Server

- Application: OpenSSL

# 6 Detailed Test Cases

## *6.1 Test Cases*

### 6.1.1 FCS_HTTPS_EXT.1.1 Test 1

| Table 2 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Attempt to establish an HTTPS connection with a server<br>• Observe the traffic with a packet analyzer<br>• 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 3 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **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 4 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Determine that the user is notified of the certificate validation failure<br>• Load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function<br>• Demonstrate that the function succeeds<br>• 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 5 – FCS_RBG_EXT.1.1 TSS** | |
|---|---|
| If use no DRBG functionality is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services | |
| **Evaluator Findings** | The evaluator inspected the application and its developer documentation to verify that the application needs no random bit generation services. The TOE itself, ST, and AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that the only cryptographic functionality used by the TOE is TLS. The TLS stack is completely provided by the platform OS. The TOE itself does not provide any services that requires random bits.<br><br>Based on these findings, this activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.5 FCS_STO_EXT.1.1 TSS

| **Table 6 – 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.<br><br>Based on these findings, this activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.6 FCS_STO_EXT.1.1 Test 1

| **Table 7 – 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.<br>For iOS: The evaluator shall verify that all credentials are stored within a Keychain. |
| **Pass/Fail Explanation** | The Apple iOS 11 Contacts 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

| **Table 8 – 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 9 – 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 “Secure Communications,” 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.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.9 FCS_TLSC_EXT.1.1 Test 1

| **Table 10 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Configure a server to accept one ciphersuite at a time<br>• Connect to the server<br>• Repeat for each ciphersuite<br>• 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 11 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a certificate missing the Server Authentication purpose in the extendedKeyUsage field<br>• Connect to a server using the certificate<br>• 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 12 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a server that sends a server certificate that does not match the server-selected ciphersuite<br>• 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 13 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a server that sends a TLS_NULL_WITH_NULL_NULL ciphersuite<br>• Attempt to connect to the server<br>• 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 14 – 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:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Make various modification to traffic as required<br>• 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 (Selection Based Requirement)

| **Table 15 – 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.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.15 FCS_TLSC_EXT.1.2 Guidance (Selection Based Requirement)

| **Table 16 – 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 that pre-installed in the iOS Trust Store and that no configuration (including setting reference identifiers) are required.<br><br>Based on this the assurance activity is considered satisfied. |

| | |
|---|---|
| Verdict | Pass |

### 6.1.16 FCS_TLSC_EXT.1.2 Test 1 (Selection Based Requirement)

| Table 17 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **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<br>• Attempt to connect to the server<br>• 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 (Selection Based Requirement)

| Table 18 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **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<br>• Attempt to connect to the server<br>• 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 (Selection Based Requirement)

| Table 19 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension<br>• Attempt to connect to the server<br>• 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 (Selection Based Requirement)

| Table 20 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension<br>• Attempt to connect to the server<br>• 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 (Selection Based Requirement)

| Table 21 – 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 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.<br>• 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.<br>• 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.<br>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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Set up server with a variety of server certificates created to reflect the condition specified in each of the tests<br>• 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 (Selection Based Requirement)

| Table 22 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Attempt to connect to a peer using a certificate without a valid certification path<br>• This results in an authenticate failure<br>• Load the trusted CA certificate(s) needed to validate the peer's certificate<br>• Demonstrate that the connection succeeds |

| | |
|---|---|
| | • Delete one of the CA certificates<br>• 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 23 – 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,<br>• secp256r1<br>• secp384r1<br>The evaluator also found that these curves are supported by default and no configuration is required.<br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.23 FCS_TLSC_EXT.4.1 Guidance

| **Table 24 – 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 “Secure Communications,” to determine the verdict of this activity. Upon investigation, the evaluator found that no configuration required which is consistent with the ST.<br>Based on these findings, this Assurance Activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.24 FCS_TLSC_EXT.4.1 Test 1

| **Table 25 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |

| | |
|---|---|
| **Test Flow** | • Configure a server to perform ECDHE key exchange using each of the TOE's supported curves<br>• 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 26 – 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,<br>• Network Connectivity<br>• Camera<br>• Location Services<br>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.<br>Based on these finds, this activity is considered satisfied. |
| **Verdict** | Pass |

### 6.1.26 FDP_DEC_EXT.1.1 Test 1

| **Table 27 – 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,<br>• Network Connectivity<br>• Camera<br>• Location Services<br>This list is consistent with the list presented in the ST. Additionally, the TOE itself provides an identification that both Location and Camera are being accessed upon use. This was demonstrated via testing, as described below.<br>Based on these findings, this activity is considered satisfied. |

| | |
|---|---|
| **Test Flow** | • Start Contacts<br>• Open any existing contact<br>• Click on Edit -> Add Photo<br>• Click on Share my Location |
| **Pass/Fail Explanation** | Contacts provides the user with a list of required hardware resources. This meetings the testing requirements. |
| **Result** | Pass |

### 6.1.27 FDP_DEC_EXT.1.2 Guidance

| **Table 28 – 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 respository which it accesses, identify the justification as to why access is required.<br>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 verified that either the application software or its documentation provides a list of the sensitive information repositories it accesses. AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that section 4 of AGD identifies that the following sensitive information repositories are accessed by the TOE,<br>• Address Book<br>This is consistent with the access described in ST. Additionally, the evaluator found that section 4 of AGD provides a justification for why access to the Address Book is required. Specifically, access is required because providing users access to the address book is the core functionality of the application.<br>Based on these findings, this activity is considered satisfied. |
| **Result** | Pass |

### 6.1.28 FDP_NET_EXT.1.1 Test 1

| **Table 29 – 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 |
| **Test Flow** | • Initialize the application<br>• Open an existing contact and scroll down to bottom.<br>• Click on “Share Location for one hour”<br>• The above action will trigger Network Activity and will be captured in wireshark. |
| **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 30 – 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 <IP-Address> prior to exercising the application<br>• Initialize and engage with the application to perform some activity.<br>• Execute nmap <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_DAR_EXT.1.1 TSS 1

| Table 31 – 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:<br>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 each contact is stored on the platform for use by the application is stored under Class C (Protected Until First User Authentication- NSFileProtectionComplete). No other files are stored by the application.<br><br>Based on these findings, this activity is considered satisfied. |
| **Verdict** | Pass |

## *6.2* Test Cases (Identification and Authentication)

### 6.2.1 FIA_X509_EXT.1.1 TSS (Selection Based Requirement)

| Table 32 – 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.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.2.2 FIA_X509_EXT.1.1 Test 1 (Selection Based Requirement)

| **Table 33 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Attempt to connect to a peer using a certificate without a valid certification path<br>• This results in an authenticate failure<br>• Load the trusted CA certificate(s) needed to validate the peer's certificate<br>• Demonstrate that the connection succeeds<br>• Delete one of the CA certificates<br>• 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 |

### 6.2.3 FIA_X509_EXT.1.1 Test 2 (Selection Based Requirement)

| **Table 34 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Change the time on the platform to a time in the future (when the server certificate is expired)<br>• 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 |

### 6.2.4 FIA_X509_EXT.1.1 Test 3 (Selection Based Requirement)

| **Table 35 – 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.<br>• The evaluator shall test revocation of the node certificate<br>• 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.<br>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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Make a connection<br>• Ensure that a valid certificate is used, and that the validation function succeeds<br>• Attempt the test with a certificate that has been revoked.<br>• 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 |

### 6.2.5 FIA_X509_EXT.1.1 Test 4 (Selection Based Requirement)

| **Table 36 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **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 |

### 6.2.6 FIA_X509_EXT.1.1 Test 5 (Selection Based Requirement)

| **Table 37 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Modify any byte in the first eight bytes of the certificate<br>• 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 |

### 6.2.7 FIA_X509_EXT.1.1 Test 6 (Selection Based Requirement)

| **Table 38 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Modify any bit in the last byte of the certificate<br>• 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 |

### 6.2.8 FIA_X509_EXT.1.1 Test 7 (Selection Based Requirement)

| **Table 39 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Modify any byte in the public key of the certificate<br>• 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 |

### 6.2.9 FIA_X509_EXT.1.2 Test 1 (Selection Based Requirement)

| **Table 40 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a certificate that does not contain the basicConstraints extension<br>• 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 |

### 6.2.10 FIA_X509_EXT.1.2 Test 2 (Selection Based Requirement)

| **Table 41 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Test Flow** | • Create a certificate of the CA issuing the TOE's certificate has the CA flag in the basicConstraints extension not set<br>• 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 |

### 6.2.11 FIA_X509_EXT.1.2 Test 3 (Selection Based Requirement)

| **Table 42 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Execution Output** | 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 |

### 6.2.12 FIA_X509_EXT.2.2 TSS (Selection Based Requirement)

| **Table 43 – 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.<br>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 and section 3.2, title “Digital Certificates,” of AGD were used to determine the verdict of this activity. Upon investigation, the evaluator found that the TOE leverages "Trusted" digital certificates that pre-installed in the iOS Trust Store. The TOE does not leverage any other certificates for connections.<br><br>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 the TOE receives its peer X.509 certificate during the initial establishment of a TLS connection. If during the revocation check of this certificate, the OCSP server cannot be contacted, the connection will not be established.<br><br>Finally, since this is the only usage of certificates by the TOE, no distinction between trusted channels is required.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.2.13 FIA_X509_EXT.2.2 Test 1 (Selection Based Requirement)

| **Table 44 – 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 VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Execution Output** | This test was covered by X509_EXT.1.1_TEST 3. |
| **Result** | Pass |

#### 6.2.14 FIA_X509_EXT.2.2 Test 2 (Selection Based Requirement)

| **Table 45 – FIA_X509_EXT.2.2 Test 2** | |
|---|---|
| **Item** | **Data/Description** |
| **Test ID** | FIA_X509_EXT.2.2_T2 |
| **Objective** | Test 2: The evaluator shall demonstrate that an invalid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity cannot be accepted. |
| **Note** | This test case leverages the testing which has previously been vetted and approved as part of VID10851. This approach has been vetted by the NIAP/NIAP validators as part of synch meeting #1 for this validation. |
| **Execution Output** | This test was covered by X509_EXT.1.1_TEST 3. Certificate validation is required. All certs are rejected unless an OSCP response is received, which requires communicating with a non-TOE entity. |
| **Result** | Pass |

### *6.3* Test Cases (Security Management)

#### 6.3.1 FMT_MEC_EXT.1.1 TSS

| **Table 46 – 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 examined the TSS of ST to determine the TOE maintains a restricted configuration with no management functions being performed by users and all configuration options are set by the underlying platform.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.3.2 FMT_MEC_EXT.1.1 Test 1

| Table 47 – 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 in to the device<br>• Execute commands to verify the defaults used by the TOE<br>• Verify that user defaults system is used to store settings |
| **Pass/Fail Explanation** | The TOE uses user defaults system for storing all settings. This meets the testing requirements. |
| **Result** | Pass |

### 6.3.3 FMT_CFG_EXT.1.1 TSS

| Table 48 – 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 |

### 6.3.4 FMT_CFG_EXT.1.1 Test 1

| Table 49 – 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 |

### 6.3.5 FMT_CFG_EXT.1.1 Test 2

| Table 50 – 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 |

### 6.3.6 FMT_CFG_EXT.1.1 Test 3

| Table 51 – 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 |

### 6.3.7 FMT_CFG_EXT.1.2 Test 1

| Table 52 – 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.<br>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 contacts. The method for verifying the permissions are enforces on the platform is to ensure that the access is as expected per the "Protected Until First User Authentication" Data Protection Class. |
| **Test Flow** | • Lock the device and call from a different device.<br>• Only the Contact Number will be shown.<br>• Unlock the device and lock it again (Class C protection triggered)<br>• Now call from telephone again.<br>• This time, Name along with Contact Number will be displayed. |
| **Pass/Fail Explanation** | Apple iOS Contacts implements Data Protection class C or "Protected Until First User Authentication" to protect its files. |
| **Result** | Pass |

### 6.3.8 FMT_SMF.1.1 Guidance

| Table 53 – 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 examined FMT_SMF.1 in the TSS in section 6 of ST to determine what management functions are mandated by the PP. According to FMT_SMF.1 there are no management functions that the TSF must be able to perform. |

| | |
|---|---|
| | Because of this there are no functions that must be described in the guidance and the assurance activity is considered satisfied. |
| **Verdict** | Pass |

#### 6.3.9 FMT_SMF.1.1 Test 1

| Table 54 – FMT_SMF.1.1 Test 1 | |
|---|---|
| **Item** | **Data/Description** |
| **Test ID** | FMT_SMF.1.1_T1 |
| **Objective** | The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed |
| **Pass/Fail Explanation** | “no management functions” has been selected within the SFR, therefore, no activities would be required for this testing |
| **Result** | Not Applicable |

### *6.4* Test Cases (Privacy)

#### 6.4.1 FPR_ANO_EXT.1.1 TSS

| Table 55 – 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 examined the TSS to identify functionality in the application where PII can be transmitted. Section 5.2.5 and the TSS of ST were used to determine the verdict of this activity. Upon investigation, the evaluator found that The TOE does not request any PII with the intent to transmit the data over the network.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

#### 6.4.2 FPR_ANO_EXT.1.1 Test 1

| Table 56 – 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** | The TOE does not request any PII with the intent to transmit the data over the network. Therefore, there is no functionality to exercise. This activity is satisfied trivially. |
| **Result** | Pass |

### *6.5 Test Cases (Protection of the TSF)*

#### 6.5.1 FPT_API_EXT.1.1 TSS

| Table 57 – 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:<br>• Accounts.framework<br>• AddressBook.framework<br>• AppKit.framework<br>• AppSupport.framework<br>• AssistantServices.framework<br>• Contacts.framework<br>• ContactsDonation.framework<br>• CoreData.framework<br>• CoreFoundation.framework<br>• CoreGraphics.framework<br>• CoreSpotlight.framework<br>• CoreSuggestions.framework<br>• CoreText.framework<br>• DataAccessExpress.framework<br>• Foundation.framework<br>• IntlPreferences.framework<br>• PhoneNumber.framework<br>• Security.framework<br>• TCC.framework<br>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.<br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.5.2 FPT_AEX_EXT.1.1 TSS

| **Table 58 – 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.<br>Based on these findings, this assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.5.3 FPT_AEX_EXT.1.1 Test 1

| Table 59 – 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.<br>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 Contacts.<br>• ssh into the device.<br>• Execute command: kill -s ABRT <PID><br>• Repeat the above two steps, thrice.<br>• Save the logs.<br>• Verify that Contacts 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 |

### 6.5.4 FPT_AEX_EXT.1.2 Test 1

| Table 60 – 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.<br>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 Contacts.<br>• ssh into the device.<br>• Execute command: kill -s ABRT <PID><br>• 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 |

### 6.5.5 FPT_AEX_EXT.1.3 Test 1

| Table 61 – 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:<br>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<br>• Initialize and engage the application. |
| **Pass/Fail Explanation** | Contacts is shipped with iOS and hence the software version for Contacts will be the same as that of iOS version. The tester observed that Contacts was able to successfully run on the certified version of the TOE platform. This meets the test requirements. |
| **Result** | Pass |

### 6.5.6 FPT_AEX_EXT.1.4 Test 1

| **Table 62 – 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:<br>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 |

### 6.5.7 FPT_AEX_EXT.1.5 TSS

| **Table 63 – 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.<br><br>Based on this, the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### 6.5.8 FPT_AEX_EXT.1.5 Test 1

| **Table 64 – 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:<br>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/Contacts.app<br>• Run the Tool to verify that –fstack –protector –all is used<br>  • Execute command: otool -lv Contacts \| grep stack<br>• 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 |

### 6.5.9 FPT_TUD_EXT.1 Test 1

| **Table 65 – 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 (https://www.apple.com/business/docs/iOS_Security_Guide.pdf) and verify what the description of Contacts distribution<br>• Verify the current version and if there if there is a new version available<br>  • Tap “Settings”<br>  • Tap “General” |
| **Pass/Fail Explanation** | The TOE leverages the defined update mechanisms and does not issue an error. This testing requirement is considered satisfied. |
| **Result** | Pass |

### 6.5.10 FPT_TUD_EXT.1.2 Test 1

| **Table 66 – 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:<br>For iOS: The evaluator shall ensure that the application is packaged in the IPA format. |
| **Test Flow** | • Navigate to the Apple App Store<br>• Verify the TOE is included in the App Store (ensuring that it’s an IPA file) |
| **Pass/Fail Explanation** | The TOE is found on the Apple App Store ensuring that it is an IPA file. This meets the testing requirements. |
| **Result** | Pass |

### 6.5.11 FPT_TUD_EXT.1.3 Test 1

| **Table 67 – 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 |

### 6.5.12 FPT_TUD_EXT.1.4 Test 1

| Table 68 – 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** | • Examine the file system for files related to the application<br>• Use the application<br>• Re-Examine the file system for files related to the application and verify that have not changed |
| **Pass/Fail Explanation** | The TOE does not modify any executable files. This meets the testing requirements. |
| **Result** | Pass |

### 6.5.13 FPT_TUD_EXT.1.5 Test 1

| Table 69 – 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 |
| **Test Flow** | • Review iOS Security Guide (https://www.apple.com/business/docs/iOS_Security_Guide.pdf)<br>• Go to “Settings” -> “About” and verify the software version. |
| **Pass/Fail Explanation** | The installed version of the software matches the expected version of the software. This meets the testing requirements. |
| **Result** | Pass |

### 6.5.14 FPT_TUD_EXT.1.6 TSS

| Table 70 – 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. 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.<br><br>Based on these findings, this activity is considered satisfied. |
| **Verdict** | Pass |

#### 6.5.15 FPT_LIB_EXT.1 Test 1

| **Table 71 – 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<br>• Execute the command: ls -alR <application directory> (This will show everything installed)<br>• 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 |

### *6.6 Test Cases (Trusted Path)*

#### 6.6.1 FTP_DIT_EXT.1 Test 1

| **Table 72 – 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 |
| **Test Flow** | • Initialize the application<br>• Open an existing contact and scroll down to bottom.<br>• Click on “Share Location for one hour”<br>• The above action will trigger Network Activity and will be captured in wireshark. |
| **Pass/Fail Explanation** | The TOE only sends user initiated TLS traffic as expected. This meets the testing requirements. |
| **Result** | Pass |

### 6.6.2 FTP_DIT_EXT.1 Test 2

| Table 73 – 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 the application<br>• Open an existing contact and scroll down to bottom.<br>• Click on “Share Location for one hour”<br>• The above action will trigger Network Activity and will be captured in wireshark.<br>• Verify that all traffic from the TOE is TLS encrypted and no sensitive traffic is output |
| **Pass/Fail Explanation** | The TOE does not send sensitive data in plaintext. This meets the testing requirements. |
| **Result** | Pass |

### 6.6.3 FTP_DIT_EXT.1 Test 3

| Table 74 – 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 75 – 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 76 – 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.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

## 7.3 AGD_OPE.1 Guidance 2

| Table 77 – 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 78 – 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 VID10851. This is VID of the platform the TOE resides within.<br><br>Based on this the assurance activity is considered satisfied. |
| Verdict | Pass |

### *7.5 ALC_CMC.1 ST*

| **Table 79 – 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 11 Contacts on iPhone and iPad. This is consistent with how the product is identified in the guidance document and on Apple Software's product website.<br><br>Based on this the assurance activity is considered satisfied. |
| **Verdict** | Pass |

### *7.6 ALC_CMS.1 Guidance*

| **Table 80 – 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.<br><br>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 81 – 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 82 – 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.<br><br>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 83 – 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.<br>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.<br>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.<br>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.<br>Based on these findings, this work unit is considered satisfied. |
| **Verdict** | Pass |

### *7.10* AVA_VAN.1 Test 1

| **Table 84 – 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.<br>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.<br><br>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.<br><br>• General web search<br>• http://nvd.nist.gov/<br>• https://www.exploit-db.com/search<br>• www.securityfocus.com<br>The evaluator performed the public domain vulnerability searches using the following key words on 8/2/18 and 8/31/2018.<br><br>• Apple iOS Contacts<br>• Apple Framework<br>• Contacts<br>• Apple iOS Contacts<br>• Apple Framework<br>• Contacts<br>• Apple iOS 11<br>• Apple CoreCrypto Kernel Module<br>• Apple CoreCrypto Module<br><br>The evaluator selected the search key words based upon the following criteria.<br><br>• The vendor name was searched,<br>• The product name was searched, |

| | |
|---|---|
| | • Key platform features the product leverages were searched<br>The search returned no applicable vulnerabilities. |
| **Verdict** | Pass |

### *7.11 AVA_VAN.1 Test 2*

| **Table 85 – 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 LiveSafe version 16.0 |
| **Test Flow** | • Scan the TOE with a virus scanner<br>• 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---**