Assurance Activity Report for Apple iOS and iPadOS 13 Contacts

Apple iOS and iPadOS 13 Contacts Security Target
Version 1.2

Application Software Protection Profile, version 1.3

AAR Version 1.5, June 2020

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Apple Inc.

The Author of the Security Target:
Acumen Security, LLC.

The TOE Evaluation was Sponsored by:
Apple Inc.

Evaluation Personnel:

Rutwij Kulkarni

Danielle Canoles

Kenji Yoshino

Acumen Security LLC

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
0.1	April 2020	Initial Release
1.0	April 2020	Updated based on review
1.1	May 2020	Updated for submission
1.2	May 2020	Updated based on ECR comments
1.3	May 2020	Updated based on ECR comments
1.4	June 2020	Updated based on equivalency and vulnerability search updates
1.5	June 2020	Updated for publication

Table of Contents

1 TOE Overview

The TOE is the Apple iOS and iPadOS 13 Contacts application which runs on iPhones and iPads. The product provides access and management of user contact information within the devices.

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

1.1 TOE Description

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

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

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11 Pro	A2160 A2215 A2216 A2217	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone 11	A2111 A2221 A2222 A2223	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone SE (2nd Gen)	A2275 A2296 A2298	iOS	A13 Bionic	802.11a/b/g/n/ac/ax	5.0
iPhone Xs Max	A1921 A2101 A2102 A2103 A2104	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone Xr	A1984 A2105 A2106 A2107 A2108	iOS	A12 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPhone X	A1865 A1901 A1902 A1903	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 8	A1863 A1905 A1906 A1907	iOS	A11 Bionic	802.11a/b/g/n/ac	5.0
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 7	A1660 A1778 A1779 A1780	iOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPhone 6s Plus	A1634 A1687 A1690 A1699	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone 6s	A1633 A1688 A1691 A1700	iOS	A9	802.11a/b/g/n/ac	4.2
iPhone SE	A1662 A1723 A1724	iOS	A9	802.11a/b/g/n/ac	4.2
iPad Pro 12.9-inch (4th gen)	A2229 A2232 A2069 A2233	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 11-inch (2nd gen)	A2228 A2068 A2230 A2331	iPadOS	A12Z Bionic	802.11a/b/g/n/ac/ax	5.0
iPad Pro 12.9-inch (3rd gen)	A1876 A1895 A1983 A2014	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	OS	Processor	WiFi	Bluetooth
iPad Pro 11-inch	A1980 A1934 A1979 A2013	iPadOS	A12X Bionic	802.11a/b/g/n/ac	5.0
iPad Air (3rd gen)	A2123 A2152 A2153 A2154	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad mini (5th gen)	A2124 A2125 A2126 A2133	iPadOS	A12 Bionic	802.11a/b/g/n/ac	5.0
iPad Pro 12.9” (2nd Gen)	A1670 A1671 A1821	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad Pro 10.5”	A1701 A1709 A1852	iPadOS	A10X Fusion	802.11a/b/g/n/ac	4.2
iPad 10.2”	A2198 A2199 A2200	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad 9.7”	A1893 A1954	iPadOS	A10 Fusion	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (1st Gen)	A1584 A1652	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad Pro 9.7”	A1673 A1674 A1675	iPadOS	A9X	802.11a/b/g/n/ac	4.2
iPad (5th gen)	A1822 A1823	iPadOS	A9	802.11a/b/g/n/ac	4.2
iPad Air 2	A1566 A1567	iPadOS	A8X	802.11a/b/g/n/ac	4.2
iPad mini 4	A1538 A1550	iPadOS	A8	802.11a/b/g/n	4.2

Table 1 IT Environment Components

2 Security Functional Requirement Identification

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

Requirement	Description
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_STO_EXT.1	Storage of Credentials
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_IDV_EXT.1	Software Identification and Versions
FTP_DIT_EXT.1	Protection of Data in Transit

Table 2 Included SFRs

3 Equivalency Analysis

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

3.1 Platform/Hardware Dependencies

The underlying HW platforms differ in SoC, RAM, storage, Screen size, and Wireless connectivity supported.

The platforms on which the TOE resides contain one of eleven SoCs:

- Apple A13
- Apple A12
- Apple A12X
- Apple A12Z[1]
- Apple A11
- Apple A10X
- Apple A10
- Apple A9X
- Apple A9
- Apple A8X
- Apple A8

While architecturally similar, the SoCs do contain differences; however, these differences do not affect the TOE functionality. All SoCs are use the ARMv8 architecture and implement the 64-bit A64 instruction set. The older processors also support the 32-bit A32 instruction set; however, the TOE is a 64-bit application regardless of processor. The SoCs also differ in the number of CPU and GPU cores, but all SoCs contain at least two CPU cores. The differences in CPU cores affects performance, but not the function of the TOE. The GPU cores are accessed through platform frameworks that abstract any differences from the application.

The amount of RAM, amount of storage, screen size, and wireless connectivity do not affect the operation of the TOE.

3.2 Software/OS Dependencies:

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 13.4.1 or iPadOS version 13.4.1. Both OSs provide the same core functionality:

1. TLS functionality
2. Application sandboxing,
3. DRBG,
4. Encrypt sensitive data,
5. X.509 certificate validation

[1] The A12Z is considered the same CPU as the A12X. The only difference between the SoCs is an additional GPU core in the A12Z.

The iPadOS features not present in iOS and iPadOS are highlighted below. Note that these differences do not affect the TOE functionality.

- Multitasking,
- Sidecar – where the user can use the iPad as an Extended display,
- Trackpad support

3.3 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical including the version of the library. There are no differences between the included libraries.

3.4 TOE Functional Differences

The TOE is a software application. There are no differences in TOE functionality based on the underlying OS or platform.

3.5 Test Subset Justification/Rationale

Apple iOS and Apple iPadOS provide the same core functionality. The SoCs also provide the same execution environment for the TOE to run in.

The test subset was determined by the following factors:

1. There are minor SoC differences that should not affect the operation of the TOE.
2. Apple iOS and Apple iPadOS contain differences; however, the differences should not affect the operation of the TOE.
3. The TOE software binary the same for all platforms and OSs.
4. The TOE functionality on iOS and iPadOS is the same.

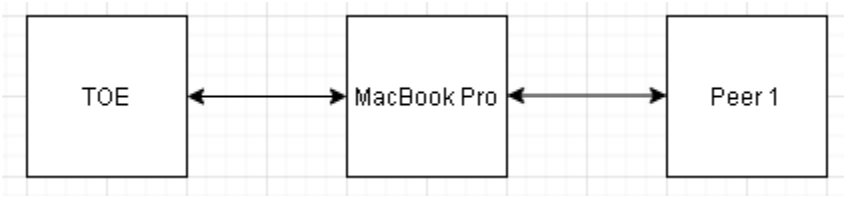
Based on the above factors, Acumen Security tested the TOE on the oldest and newest CPUs as well as on iOS and iPadOS.

Device	CPU Model	Operating System
iPad Mini 4	A8	Apple iPadOS
iPhone 6s	A9	Apple iOS
iPad Pro 11 inch	A12X	Apple iPadOS
iPhone 11	A13	Apple iOS

4 Test Diagram

- **Testing Location:**
  - Acumen Security, 2400 Research Boulevard Rockville Maryland, 20850
  - One Apple Parkway, Cupertino, CA 95014

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



- TOE
  - Version: Apple Contacts 13.4.1
  - Platform OS: iOS/iPadOS 13.4.1
  - HW Platform: iPhone 6s, iPhone 11, iPad mini 4, iPad Pro 11 inch
  - IP Address: HW Platform Dependent
  - MAC address: HW Platform Dependent
  - Protocols: TLS v1.2, HTTPS
  - Time: Set Manually and verified
- Apple MacBook Pro
  - Name: Apple MacBook Pro 2018
  - Software Version: Apple macOS Catalina 10.15
  - Role: Router
  - Internet connection is shared from MacBook Pro via USB to the TOE for tests:
    - FDP_NET_EXT.1.1_T2 and
    - FTP_DIT_EXT.1.1_T2
  - Tools: Wireshark v2.6.9, OpenSSH v7.9p1, Quick time Player v10.15, nmap v 7.80
  - Time: Set Manually and verified
  - Packet captures were performed on Apple MacBook Pro 2018
- Peer 1
  - Test: FTP_DIT_EXT.1.1 T2
  - Protocols: TLS v1.2, HTTPS
  - Sub-Domain: p11-contacts.icloud.com, p18-contacts.icloud.com, contacts.fe.apple-dns.net

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Cryptographic Support)

5.1.1 FCS_RBG_EXT.1

5.1.1.1 FCS_RBG_EXT.1.1 TSS

Objective	If **use no DRBG functionality** is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.
Evaluator Findings	The evaluator found that the TSS in section 6 'TOE Summary Specification', specifically the FCS_RBG_EXT.1 entry of Table 11, states: "The TOE does not use DRBG functionality." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FCS_CKM_EXT.1

5.1.2.1 FCS_CKM_EXT.1.1 TSS

Objective	The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the **generate no asymmetric cryptographic keys** selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.
Evaluator Findings	The evaluator found that the TSS in section 6 'TOE Summary Specification', specifically the FCS_CKM_EXT.1 entry of Table 11, states: "The TOE does not perform asymmetric key generation." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FCS_STO_EXT.1

5.1.3.1 FCS_STO_EXT.1.1 TSS

Objective	The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.
Evaluator Findings	The evaluator checked the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. The TSS in section 6 'TOE Summary Specification' FCS_STO_EXT.1 entry of Table 11 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. Based on these findings, this activity is considered satisfied.

Verdict	Pass

5.1.4 FDP_DEC_EXT.1

5.1.4.1 FDP_DEC_EXT.1.1 Guidance

Objective	The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator verified that either the application software or its documentation provides a list of the hardware resources it accesses. AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that section 4 titled 'Resource Usage' of AGD identifies that the following hardware resources are accessed by the TOE, • Network Connectivity: This is required for Contacts to facilitate communications with remote Apple Servers or other user configured servers. • Camera: This is required for Contacts to associate a picture with contacts. This is consistent with the access described in ST. Additionally, the evaluator found that section titled 'Resource Usage' of AGD provides a justification for why access to Network Connectivity and the Camera are required. Based on these findings, this activity is considered satisfied.
Result	Pass

5.1.4.2 FDP_DEC_EXT.1.2 Guidance

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

	Based on these findings, this activity is considered satisfied.
Result	Pass

5.1.5 FDP_DAR_EXT.1

5.1.5.1 FDP_DAR_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS. If **not store any sensitive data** is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below.
Evaluator Findings	The evaluator inspected the TSS and 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 in section 6 'TOE Summary Specification' FDP_DAR_EXT.1 entry of Table 11 of the 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. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Security Management)

5.2.1 FMT_MEC_EXT.1

5.2.1.1 FMT_MEC_EXT.1.1 TSS (TD0437)

Objective	The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.
Evaluator Findings	The evaluator examined the TSS in section 6 'TOE Summary Specification' FMT_MEC_EXT.1 entry in Table 11 of the ST to determine the TOE maintains a restricted configuration with no management functions being performed by users and all configuration options are set by the underlying platform. Based on this the assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FMT_CFG_EXT.1

5.2.2.1 FMT_CFG_EXT.1.1 TSS

Objective	The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.
Evaluator Findings	The evaluator examined the TSS section 6 'TOE Summary Specification' FMT_CFG_EXT.1 entry in Table 11 of the ST to determine if the application requires any credentials and if it installs with default credentials. Section 6 of the ST was used to determine the verdict of this assurance activity. The evaluator found that the TOE does not come with any default credentials. The user must configure an account first before accessing the TOE and underlying platform. Based on this the evaluation is considered satisfied.
Verdict	Pass

5.2.3 FMT_SMF.1

5.2.3.1 FMT_SMF.1.1 Guidance

Objective	The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Evaluator Findings	The evaluator examined FMT_SMF.1 in the TSS in section 6 of 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

5.3 TSS and Guidance Activities (Privacy)

5.3.1 FPR_ANO_EXT.1

5.3.1.1 FPR_ANO_EXT.1.1 TSS

Objective	The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.
Evaluator Findings	The evaluator examined the TSS section 6 'TOE Summary Specification' FPR_ANO_EXT.1 entry in Table 11 of the ST 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 will transmit user contact information. Additionally, the evaluator found that a notification is provided prior to this transmission. Based on this the assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (Protection of the TSF)

5.4.1 FPT_API_EXT.1

5.4.1.1 FPT_API_EXT.1.1 TSS

Objective	The evaluator shall verify that the TSS lists the platform APIs used in the application.
Evaluator Findings	The evaluator examined the TSS section 6 'TOE Summary Specification' FPT_API_EXT.1 entry in Table 11 of the ST to determine if the platform APIs used in the application are listed. Upon investigation, the evaluator found that TSS lists the platform APIs used by the TOE. Based on this the assurance activity is considered satisfied.
Verdict	Pass

5.4.2 FPT_AEX_EXT.1

5.4.2.1 FPT_AEX_EXT.1.1 TSS

Objective	The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.
Evaluator Findings	The evaluator examined the TSS section 6 'TOE Summary Specification' FPT_AEX_EXT.1 entry in Table 11 of the ST to determine if it describes the compiler flags used to enable ASLR. The TSS of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE is compiled with ASLR enabled. This is accomplished by being compiled with the -fPIE flag. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3 FPT_TUD_EXT.1

5.4.3.1 FPT_TUD_EXT.1.1 Guidance

Objective	The evaluator shall check to ensure the guidance includes a description of how updates are performed.
Evaluator Findings	The evaluator checked section 2 'Installation/Update' of the AGD which describes how updates are performed in detail.
Verdict	Pass

5.4.3.2 FPT_TUD_EXT.1.2 Guidance

Objective	The evaluator shall verify guidance includes a description of how to query the current version of the application.
Evaluator Findings	The evaluator verified section 2.1 'Verifying Product Version' of the AGD describes detailed instructions on how to query the current version of the application.
Verdict	Pass

5.4.4 FPT_TUD_EXT.1

5.4.4.1 FPT_TUD_EXT.1.4 TSS

Objective	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 'TOE Summary Specification' FPT_TUD_EXT.1 entry in Table 11 of the ST and the guidance document (section 2 'Installation/Update') were used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE is provided within the underlying OS image and packaged as a signed IPA file. iOS considers the signature authorized if the certificate used to sign the IPA file chains to the Apple Worldwide Developer Relations Certification Authority or the Apple iPhone Certification Authority. Updates to the TOE are provided through underlying OS updates and current versions of the TOE can be checked through the Settings of the underlying platform. The ST (TSS) and the AGD are adequately consistent to ensure that they both describe how candidate updates are obtained. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.5 FPT_TUD_EXT.1

5.4.5.1 FPT_TUD_EXT.1.5 TSS

Objective	The evaluator shall verify that the TSS identifies how the application is distributed.
Evaluator Findings	The evaluator examined the TSS to determine if it identifies how the application is distributed. Section 6 'TOE Summary Specification' FPT_TUD_EXT.1 entry in Table 11 of the ST was 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." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.6 FPT_IDV_EXT.1

5.4.6.1 FPT_IDV_EXT.1 TSS

Objective	If "other version information" is selected the evaluator shall verify that the TSS contains an explaination of the versioning methodology.
Evaluator Findings	The evaluator checked the TSS in section 6 'TOE Summary Specification' FPT_IDV_EXT.1 entry in Table 11 of the ST which contains an explanation of the versioning methodology and was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states:

	"Each iOS and iPadOS application must be distributed in as an Application Bundle. The Application Bundle includes an Info.plist file containing the following identifying information: Bundle name, Bundle ID, and Platform version (since the TOE is included with the platform OS). For the TOE, these are the following key/value pairs in the Info.plist file: • Bundle name: Contacts • Bundle identifier: com.apple.MobileAddressBook • DTPlatformVersion: 13.4.1" Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Trusted Path)

5.5.1 FTP_DIT_EXT.1

5.5.1.1 FTP_DIT_EXT.1 TSS

Objective	For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.
Evaluator Findings	The evaluator checked the TSS in section 6 'TOE Summary Specification' FPT_DIT_EXT.1 entry in Table 11 of the ST to determine if it identifies the call to invoke platform provided functionality and was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS stated that all application data is transmitted securely via platform provided HTTPS and TLS with Apple Servers or other user configured servers. The TSS also states that the NSURL class is used to invoke the HTTPS/TLS functionality. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Test Activities (Cryptographic Support)

6.1.1 FCS_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 implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1(1) or conditioned according to FCS_CKM.1.1(1) and FCS_CKM.1(3). For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform. **For iOS**: The evaluator shall verify that all credentials are stored within a Keychain.
Note	Contacts does not store credentials. Each contact is stored under Class C protection
Pass/Fail Explanation	The TOE does not store any credentials. Therefore, there is no credentials to verify. This meets the testing requirements.
Result	Pass

6.2 Test Activities (User Data Protection)

6.2.1 FDP_DEC_EXT.1.1 Test 1

Item	Data/Description
Test ID	FDP_DEC_EXT.1.1_T1
Objective	**For iOS**: The evaluator shall verify that either the application or the documentation provide the user with a list of the required hardware resources it accesses.
Test Flow	• Verify TOE documentation provides a list of required hardware resources.
Pass/Fail Explanation	This is satisfied by the FDP_DEC_EXT.1.1 Guidance Evaluation Activity.
Result	Pass

6.2.2 FDP_DEC_EXT.1.2 Test 1

Item	Data/Description
Test ID	FDP_DEC_EXT.1.2_T1
Objective	**For iOS**: The evaluator shall verify that either the application software or its documentation provides a list of the sensitive information repositories it accesses.
Test Flow	• Verify TOE documentation provides a list of required sensitive information repositories.
Pass/Fail Explanation	This is satisfied by the FDP_DEC_EXT.1.2 Guidance Evaluation Activity.
Result	Pass

6.2.3 FDP_NET_EXT.1.1 Test 1

Item	Data/Description
Test ID	FDP_NET_EXT.1.1_T1
Objective	The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user initiated
Note	This test is performed in conjunction with FTP_DIT_EXT.1 Test #2.
Test Flow	• Run the TOE and capture packets. • Identify application associated traffic. • Verify that all application network communications are documented in the TSS or are user initiated.
Pass/Fail Explanation	All TOE network communications were user-initiated. No TOE initiated network communications were observed or documented in the TSS.
Result	Pass

6.2.4 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	• TCP
	  ○ Perform a TCP port scan prior to exercising the application
	  ○ Initialize and engage with the application to perform some activity.
	  ○ Perform a TCP port scan after exercising the application
	• UDP
	  ○ Perform a UDP port scan prior to exercising the application
	  ○ Initialize and engage with the application to perform some activity.
	  ○ Perform a UDP port scan after exercising the application

Pass/Fail Explanation	The TOE did not open any ports. This meets the testing requirements.
Result	Pass

6.2.5 FDP_DAR_EXT.1.1 Test 1

Item	Data/Description
Test ID	FDP_DAR_EXT.1.1_T1
Objective	*Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1. The evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.* *If **leverage platform-provided functionality** is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis:* ***For iOS**: The evaluator shall inspect the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally.*
Test Flow	• Examine the TSS and ensure that it describes how the application uses the Complete Protection, Protected Unless Open, or Protected Until First User Authentication Data Protection Class for each data file stored locally.
Pass/Fail Explanation	This is satisfied by the FDP_DAR_EXT.1.1 TSS Evaluation Activity.
Result	Pass

6.3 Test Activities (Security Management)

6.3.1 FMT_MEC_EXT.1.1 Test 1 (TD0437)

Item	Data/Description
Test ID	FMT_MEC_EXT.1.1_T1
Objective	If “invoke the mechanisms recommended by the platform vendor for storing and setting configuration options” is chosen, the method of testing varies per platform as follows:

	For iOS: The evaluator shall verify that the app uses the user defaults system or key-value store for storing all settings.
Test Flow	• ssh into the device • Execute command: defaults read | grep com.apple.contacts • Execute command: defaults read com.apple.contactsd.BackupConfigurationService • Execute command: defaults read com.apple.contactsd.VerifyCoreSpotlightService • Execute commands: defaults read com.apple.accessoryd.plugin
Pass/Fail Explanation	The TOE uses the user defaults system for storing all settings.
Result	Pass

6.3.2 FMT_CFG_EXT.1.1 Test 1

Item	Data/Description
Test ID	FMT_CFG_EXT.1.1_T1
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail Explanation	*The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.*
Result	Pass

6.3.3 FMT_CFG_EXT.1.1 Test 2

Item	Data/Description
Test ID	FMT_CFG_EXT.1.1_T2
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available
Pass/Fail Explanation	*The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.*
Result	Pass

6.3.4 FMT_CFG_EXT.1.1 Test 3

Item	Data/Description
Test ID	FMT_CFG_EXT.1.1_T3
Objective	If the application uses any default credentials the evaluator shall run the following tests. The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.
Pass/Fail Explanation	*The TSS states that the TOE does not come with default credentials. Therefore, this test case is not applicable.*
Result	Pass

6.3.5 FMT_CFG_EXT.1.2 Test 1

Item	Data/Description
Test ID	FMT_CFG_EXT.1.2_T1
Objective	The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform. **For iOS**: The evaluator shall determine whether the application leverages the appropriate Data Protection Class for each data file stored locally.
Note	The application does not create any files that are available in the user accessible files system. Apple iOS does not allow for direct access to system files such as 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	• Reboot the device and call from a different device. • Only the contact ID (number or email address) will be shown. • Unlock the device and lock it again (Class C protection triggered) • Call again. • This time, the contact name stored in Contacts will be displayed.
Pass/Fail Explanation	The TOE implements Data Protection class C or "Protected Until First User Authentication" to protect its files.
Result	Pass

6.3.6 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	Pass

6.4 Test Activities (Privacy)

6.4.1 FPR_ANO_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPR_ANO_EXT.1.1_T1
Objective	If require user approval before executing is selected, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII.
Pass/Fail Explanation	This test is not applicable, because the ST does not select 'require user approval before executing'.
Result	Pass

6.5 Test Activities *(Protection of the TSF)*

6.5.1 FPT_API_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_API_EXT.1.1_T1
Objective	The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.
Test Flow	• Search the platform developer references for each API listed in the TSS. • Verify all APIs are supported.
Pass/Fail Explanation	All APIs used by the TOE are supported.
Result	Pass

6.5.2 FPT_AEX_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_AEX_EXT.1.1_T1
Objective	The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. **For iOS**: The evaluator shall perform a static analysis to search for any mmap calls (or API calls that call mmap), and ensure that no arguments are provided that request a mapping at a fixed address.
Test Flow	• Navigate to the Contacts source directory • Execute “pwd” to show the directory being searched • Execute “ls” to show the files being searched • Execute “grep -r mmap *” to search all source files to see if mmap is called
Pass/Fail Explanation	The TOE does not make any calls to mmap.
Result	Pass

6.5.3 FPT_AEX_EXT.1.2 Test 1

Item	Data/Description
Test ID	FPT_AEX_EXT.1.2_T1
Objective	The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform. **For iOS**: The evaluator shall perform static analysis on the application to verify that mprotect is never invoked with the PROT_EXEC permission.
Test Flow	• Navigate to the Contacts source directory • Execute “pwd” to show the directory being searched • Execute “ls” to show the files being searched • Execute “grep -r PROT_EXEC *” to search all source files to see if any functions are called with the PROT_EXEC permission

	• Verify that the PROT_EXEC permission is never used or that is never used with mprotect if it is used
Pass/Fail Explanation	The TOE does not invoke mprotect with the PROT_EXEC permission. This meets the testing requirement.
Result	Pass

6.5.4 FPT_AEX_EXT.1.3 Test 1

Item	Data/Description
Test ID	FPT_AEX_EXT.1.3_T1
Objective	The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests: **For iOS**: Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required.
Pass/Fail Explanation	Applications running on iOS cannot disable security features, therefore this requirement is met and no evaluation activity is required.
Result	Pass

6.5.5 FPT_AEX_EXT.1.4 Test 1

Item	Data/Description
Test ID	FPT_AEX_EXT.1.4_T1
Objective	The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform: **For iOS**: The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).
Pass/Fail Explanation	This requirement is implicitly met based on the Assurance Activity.
Result	Pass

6.5.6 FPT_AEX_EXT.1.5 Test 1

Item	Data/Description
Test ID	FPT_AEX_EXT.1.5_T1
Objective	The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present. Tools such as Canary Detector may help automate these activities.
Test Flow	• Verify the presence of the ___stack_chk_fail and/or ___stack_chk_guard symbols in the compiled TOE application.
Pass/Fail Explanation	The TOE contains the ___stack_chk_fail and ___stack_chk_guard symbols, indicating that the TOE was compiled with stack smashing protections. This meets the testing requirements.
Result	Pass

6.5.7 FPT_TUD_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.1.1_T1
Objective	The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.
Test Flow	• Tap “Settings” • Tap “General” • Tap “About” • Verify the current version of the platform and TOE is displayed • Tap “< General” • Tap “Software Update” • Verify the platform reports whether an update is available
Pass/Fail Explanation	The TOE platform successfully checks for updates.
Result	Pass

6.5.8 FPT_TUD_EXT.1.2 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.1.2_T1
Objective	The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.
Pass/Fail Explanation	The TOE platform displays the current version of the TOE.
Result	Pass

6.5.9 FPT_TUD_EXT.1.3 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.1.3_T1
Objective	The evaluator shall verify that the application's executable files are not changed by the application. The evaluator shall complete the following test: 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 ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.
Test Flow	• Copy the Contacts application directory from the device to the MacBook before initialization as the “Before” version • Initialize and exercise Contacts application. • Copy Contacts application directory from the device to the MacBook after as the “After” version

	• Generate a hash of each file in the Before and After application directories • diff the outputs • Verify the two outputs are the same
Pass/Fail Explanation	The TOE does not modify any executable files. This meets the testing requirements.
Result	Pass

6.5.10 FPT_TUD_EXT.1.5 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.1.5_T1
Objective	If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS.
Test Flow	• Go to Settings > General > Reset > Erase All Content and Settings • Tap Erase Now • Enter the passcode • Tap Erase iPhone/iPad • Verify the TOE is present after the erase completes
Pass/Fail Explanation	The TOE is present after performing a factory reset.
Result	Pass

6.5.11 FPT_LIB_EXT.1 Test 1

Item	Data/Description
Test ID	FPT_LIB_EXT.1_T1
Objective	The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Test Flow	• ssh into the device • Execute the command: ls -alR <application directory> (This will show everything installed) • Very 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

6.5.12 FPT_IDV_EXT.1 Test 1

Item	Data/Description
Test ID	FPT_IDV_EXT.1_T1
Objective	The evaluator shall install the application, then check for the / existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.
Test Flow	• Open and inspect Info.plist file

	• Verify the TOE is identified by the DTPlatformVersion, Bundle display name, and Bundle identifier key/value pairs
Pass/Fail Explanation	The evaluator verified that the TOE was identified correctly. This meets testing requirements.
Result	Pass

6.6 Test Activities (Trusted Path)

6.6.1 FTP_DIT_EXT.1.1 Test 1 (TD0444)

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, DTLS, SSH, or IPsec in accordance with the selection in the ST.
Note	This test is performed in conjunction with FTP_DIT_EXT.1 Test #2
Pass/Fail Explanation	All TOE communications are over HTTPS/TLS. This meets the testing requirements.
Result	Pass

6.6.2 FTP_DIT_EXT.1.1 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	• Launch Contacts • Synchronize contacts • Delete or edit a contact • Share a contact via Email and iMessage • Quit Contacts • 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.1.1 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.
Test Flow	• Search the packets captured for FTP_DIT_EXT.1.1 Test #2 for plaintext user credentials • Verify that no plaintext credentials are found
Pass/Fail Explanation	Initiation of an HTTPS/TLS connection by the TOE does not result in transmission of plaintext credentials.
Result	Pass

6.6.4 FTP_DIT_EXT.1.1 Test 4

Item	Data/Description
Test ID	FTP_DIT_EXT.1_T4
Objective	**For iOS**: If "encrypt all transmitted data" is selected, the evaluator shall ensure that the application's Info.plist file does not contain the NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys, as these keys disable iOS's Application Transport Security feature.
Test Flow	• ssh into the device • cd into Applications/Contacts.app • Open the info.plist file • Verify that the file does not contain NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys
Pass/Fail Explanation	A search for both the keywords yielded no results.
Result	Not Applicable

7 Security Assurance Requirements

7.1 ADV_FSP.1 TSS

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

7.2 AGD_OPE.1 Guidance

Objective	Some of the contents of the operational guidance will be verified by the evaluation activities in 5.1 Security Functional Requirements and

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

7.3 AGD_PRE.1 Guidance

Objective	As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.
Evaluator Findings	Section 1 of 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. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC_CMC.1 TSS

Objective	The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator

	shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.
Evaluator Findings	The evaluator examined the ST to ensure that it contains an identifier that specifically identifies the version that meets the requirement of the ST. Section 1.1 of the ST was used to determine the verdict of this assurance activity. The evaluator found that the TOE is identified as Apple iOS and iPadOS 13 Contacts. This is consistent with how the product is identified in the guidance document and on Apple Software's product website. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.5 ALC_CMS.1 TSS & Guidance

Objective	The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation. The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.
Evaluator Findings	As stated in other assurance activities, the TOE has been uniquely identified and all identifying information is consistent. The TSS in section 6 'TOE Summary Specification' FPT_AEX_EXT.1 entry listed in Table 11 of the ST identifies how

	(stack-based) buffer overflow protection is enabled. Based on this the assurance activity is considered satisfied.
Verdict	Pass

7.6 ALC_TSU_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.
Evaluator Findings	The evaluator examined the ALC_TSU_EXT.1 entry in table 11 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 5.5 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

7.7 ALC_TSU_EXT.1 TSS 2

Objective	The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days. The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.
Evaluator Findings	The evaluator verified that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third party or carrier delays in deployment. The evaluator also verified that this time is expressed in a number or range of days. The TSS and section 5.5 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". In addition the evaluator found section 6 (TSS) states "To report security or privacy issues that affect Apple products or web servers, should contact product-security@apple.com. Submissions can use Apple's Product Security PGP key

	(https://support.apple.com/en-us/HT201214) to encrypt sensitive information that is sent by email. When the email is received, Apple will send an automatic email as acknowledgment. If this email is not received, please check the email address and send again. For the protection of our customers, Apple generally does not disclose, discuss, or confirm security issues until a full investigation is complete and any necessary patches or releases are available. Apple distributes information about security issues in its products through security advisories. Users can also receive Apple security advisories through the security-announce mailing list." Based on these findings, the assurance activity is considered satisfied.
Verdict	Pass

7.8 ATE_IND.1 Test

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

	successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.
Evaluator Findings	In support of the AAs in the PP, the evaluator created a test plan. This test plan includes an equivalency argument, a description of the test infrastructure (including the host platforms), each test case, and actual results for each test case. Based on these findings, this work unit is considered satisfied.
Verdict	Pass

7.9 AVA_VAN.1 Test 1

Objective	The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The sources of the publicly available information are provided below. The following was performed on May 29, 2020. The National Vulnerability Database (NVD) was searched for publicly reported CVEs. The following components of the TOE were searched: **Component** / **CPE** Apple iOS 13.4.1 — cpe:2.3:*:apple:iphone_os:13.4.1:*:*:*:*:*:*:* Apple iOS 13.4 — cpe:2.3:*:apple:iphone_os:13.4:*:*:*:*:*:*:* Apple iOS 13.3.1 — cpe:2.3:*:apple:iphone_os:13.3.1:*:*:*:*:*:*:* Apple iPadOS 13.4.1 — cpe:2.3:*:apple:ipad_os:13.4.1:*:*:*:*:*:*:* Apple iPadOS 13.4 — cpe:2.3:*:apple:ipad_os:13.4:*:*:*:*:*:*:* Apple iPadOS 13.3.1 — cpe:2.3:*:apple:ipad_os:13.3.1:*:*:*:*:*:*:* The TOE (Application), underlying platform OS, and all platform libraries/frameworks are distributed together, and vulnerabilities are reported under the platform OS CPE. CPEs for Apple Contacts were examined and determined to be for much older versions (e.g. iOS 9).

	No publicly known vulnerabilities were discovered in the TOE version or the prior versions. Vulnerabilities were discovered in version 13.3.1; however, these vulnerabilities were fixed in version 13.4.
Verdict	Pass

7.10 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	Scanner Used: McAfee Mobile Security: Privacy App v4.2
Test Flow	• Run a security scanner • Verify no threats are detected
Pass/Fail Explanation	The security scanner did not detect any threats.
Result	Pass

8 Technical Decisions

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

Identifier	Applicable	Exclusion Rationale (if applicable)
0510 – Obtaining random bytes for iOS/macOS	No	The TOE does not obtain random bytes from the platform.
0505 – Clarification of revocation testing under RFC6066	Yes	
0498 – Application Software PP Security Objectives and Requirements Rationale	Yes	
0495 – FIA_X509_EXT.1.2 Test Clarification	No	The TOE does not directly invoke X.509 functionality.
0486 – Removal of PP-Module for VPN Clients from allowed with list	Yes	
0473 – Support for Client or Server TOEs in FCS_HTTPS_EXT	No	The TOE uses platform HTTPS, so it does not include FCS_HTTPS_EXT.1.
0465 – Configuration Storage for .NET Apps	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
0445 – User Modifiable File Definition	Yes	
0444 – IPsec selections	Yes	
0437 – Supported Configuration Mechanism	Yes	
0435 – Alternative to SELinux for FPT_AEX_EXT.1.3	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
0434 – Windows Desktop Applications Test	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
0427 – Reliable Time Source	Yes	
0416 – Correction to FCS_RBG_EXT.1 Test Activity	Yes	

9 Conclusions

All testing and assurance activities pass.

---End of Document---