Apple iOS 12 Contacts Security Target

Acumen Security, LLC.

Table of Contents

Revision History

Version	Date	Description
0.1	November 2018	Initial Draft
0.2	November 2018	Updated based on internal review
0.3	January 2019	Updated based on Validator review.
1.0	February 2019	Updated based on ECR comments.
1.1	March 2019	Removed A7 based platforms.

1. Security Target Introduction

1.1. Security Target and TOE Reference

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

Category	Identifier
ST Title	Apple iOS 12 Contacts Security Target
ST Version	1.1
ST Date	March 2019
ST Author	Acumen Security, LLC.
TOE Identifier	Apple iOS 12 Contacts on iPhone and iPad Note: The TOE is the Contacts software only. The Apple iOS operating system has been separately validated (VID 10937).
TOE Software Version	12
TOE Developer	Apple Inc.
Key Words	Application, Mobility

Table 1 TOE/ST Identification

1.2. TOE Overview

The TOE is the Apple iOS 12 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 10937).

1.3. 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 10937). The mobile operating system and hardware platforms are part of the TOE environment. The evaluated version of the TOE is version 12.

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

Device Name	Model	Processor	WiFi	Bluetooth
iPhone XS	A1920 A2097 A2098 A2099 A2100	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XS Max	A1921 A2101 A2102 A2103 A2104	A12 Bionic	802.11a/b/g/n/ac	5.0
iPhone XR	A1984	A12 Bionic	802.11a/b/g/n/ac	5.0

Device Name	Model	Processor	WiFi	Bluetooth
	A2105 A2106 A2107 A2108			
iPhone X	A1901 A1902 A1865	A11	802.11a/b/g/n/ac	5.0
iPhone 8 Plus/ iPhone 8	A1864, A1897, A1898, A1899/ A1863, A1905, A1906, A1907	A11	802.11a/b/g/n/ac	5.0
iPhone 7 Plus/ iPhone 7	A1661, A1784, A1785, A1786/ A1660, A1778, A1779, A1780	A10	802.11a/b/g/n/ac	4.2
iPhone 6s Plus/ iPhone 6s	A1634, A1687, A1690, A1699/ A1633, A1688, A1691, A1700	A9	802.11a/b/g/n/ac	4.2
iPhone SE	A1662 A1723 A1724	A9	802.11a/b/g/n/ac	4.2
iPhone 6 Plus/ iPhone 6	A1522, A1524, A1593/ A1549, A1586, A1589	A8	802.11a/b/g/n/ac	4.0
iPad mini 4	A1538 A1550	A8	802.11a/b/g/n	4.2
iPad Air 2	A1566 A1567	A8X	802.11a/b/g/n/ac	4.2
iPad (5th gen)	A1822 A1823	A9X	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (1st Gen)	A1584 A1652	A9X	802.11a/b/g/n/ac	4.2
iPad Pro 9.7”	A1673 A1674	A9X	802.11a/b/g/n/ac	4.2
iPad Pro 12.9” (2nd Gen)	A1670 A1671	A10X	802.11a/b/g/n/ac	4.2
iPad Pro 10.5”	A1701 A1709	A10X	802.11a/b/g/n/ac	4.2
iPad 9.7”	A1893 A1954	A10	802.11a/b/g/n/ac	4.2

Table 2 Devices Covered by the Evaluation

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

1.4. TOE Architecture

1.4.1. Physical Boundaries

The TOE is a software application running on a mobile device (as listed above). The mobile device platform provides a host Operating System, controls that limit application behavior, and wireless connectivity. Note: The Apple iOS operating system has been separately validated.

1.4.2. Security Functions provided by the TOE

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

1.4.2.1. Cryptographic Support

The iOS platform provides HTTPS/TLS functionality to securely communicate with trusted entities. The TOE does not directly perform any cryptographic functions.

1.4.2.2. User Data Protection

The TOE requests no hardware or software resources during the use of the application. The TOE requires network access.

1.4.2.3. Identification and Authentication

All validation of X.509 certificates is performed by the iOS platform on which the TOE is running.

1.4.2.4. Security Management

The TOE is installed completely pre-configured. No security related configuration is required for operation.

1.4.2.5. Privacy

The TOE does not request any PII with the intent to transmit the data over the network. However, the TOE will transmit contact information at the request of the user. In these cases, the TOE provides a notification when sharing this information.

1.4.2.6. Protection of the TSF

The TOE platform performs cryptographic self-tests at startup which ensures the TOE ability to properly operate. The TOE platform also verifies all software updates via digital signature.

1.4.2.7. Trusted Path/Channels

The TOE is a software application. The TOE has the ability to establish protected communications.

1.4.3. TOE Documentation

- Apple iOS 12 Contacts Security Target, Version 1.1 [ST]
- Apple iOS 12 Contacts Common Criteria Configuration Guide, Version 1.1 [AGD]

1.4.4. Other References

Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP].

2. Conformance Claims

2.1. CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 3 extended

2.2. Protection Profile Conformance

This TOE is conformant to:

- Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP].

2.3. Conformance Rationale

This Security Target provides exact conformance to Version 1.2 of the Protection Profile for Application Software. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

2.3.1. Technical Decisions

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

Identifier	Applicable?	Exclusion Rationale (if applicable)
0385 – FTP_DIT_EXT.1 Assurance Activity Clarification	No	This TD addresses the VPN Client Module. The TOE is not claiming conformance to the VPN Client Module.
0382 – Configuration Storage Options for Apps	No	This TD modifies the Assurance Activity for the Windows and Linux platforms. The TOE runs on iOS.
0380 – Linux Keyring Requirement in FCS_STO_EXT.1	Yes	
0364 – Android mmap testing for FPT_AEX_EXT.1.1	No	This TD modifies the Assurance Activity for the Android Platform. The TOE runs on iOS.
0359 – Buffer Protection	No	This TD modifies the Assurance Activity for the Android Platform. The TOE runs on iOS.
0358 – Cipher Suites for TLS in SWApp v1.2	Yes	
0327 – Default file permissions for FMT_CFG_EXT.1.2	Yes	
0326 – RSA-based key establishment schemes	No	This TD addresses FCS_CKM.1, FCS_CKM.2, and FCS_TLSS_EXT.1.3. The TOE does not include any of these SFRs.
0305 – Handling of TLS connections with and without mutual authentication	No	This TD address the Assurance Activities associated with FCS_TLSC_EXT.2. The TOE does not include FCS_TLSC_EXT.2.
0304 – Update to FCS_TLSC_EXT.1.2	Yes	
0300 – Sensitive Data in FDP_DAR_EXT.1	Yes	
0296 – Update to FCS_HTTPS_EXT.1.3	Yes	

Identifier	Applicable?	Exclusion Rationale (if applicable)
0295 – Update to FPT_AEX_EXT.1.3 Assurance Activities	No	This TD modifies the Assurance Activity for Android/Windows Platforms. The TOE runs on iOS.
0293 – Update to FCS_CKM.1(1)	No	This TD addresses FCS_CKM.1. The TOE does not include FCS_CKM.1. Additionally, this TD has been archived.
0283 – Cipher Suites for TLS in SWApp v1.2	No	Superseded by TD0358.
0269 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on iOS. Additionally, the TD has been archived.
0268 – FMT_MEC_EXT.1 Clarification	Yes	
0267 – TLSS testing - Empty Certificate Authorities list	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0244 – FCS_TLSC_EXT - TLS Client Curves Allowed	Yes	
0241 – Removal of Test 4.1 in FCS_TLSS_EXT.1.1	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0238 – User-modifiable files FPT_AEX_EXT.1.4	Yes	
0221 – FMT_SMF.1.1 - Assignments moved to Selections	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP.
0218 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on iOS. Additionally, the TD has been archived.
0217 – Compliance to RFC5759 and RFC5280 for using CRLs	Yes	
0215 – Update to FCS_HTTPS_EXT.1.2	Yes	
0192 – Update to FCS_STO_EXT.1 Application Note	No	Superseded by TD0380
0178 – Integrity for installation tests in AppSW PP	Yes	
0177 – FCS_TLSS_EXT.1 Application Note Update	No	This TD addresses the usage of FCS_TLSS_EXT.1 as it related to FTP_DIT_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0174 – Optional Ciphersuites for TLS	No	Superseded by TD283
0172 – Additional APIs added to FCS_RBG_EXT.1.1	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on iOS.
0163 – Update to FCS_TLSC_EXT.1.1 Test 5.4 and FCS_TLSS_EXT.1.1 Test	No	This TD is only needed when DHE or ECDHE is not supported.
0131 – Update to FCS_TLSS_EXT.1.1 Test 4.5	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0122 – FMT_SMF.1.1 Assignments moved to Selections	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP. Additionally, the TD has been archived.
0121 – FMT_MEC_EXT.1.1 Configuration Options	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP.
0119 – FCS_STO_EXT.1.1 in PP_APP_v1.2	Yes	

Identifier	Applicable?	Exclusion Rationale (if applicable)
0107 – FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation	No	This TD address key generation (FCS_CKM.1). The TOE does not include key generation.

Table 3 TDs

3. Security Problem Definition

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

3.1. Threats

The following threats are drawn directly from the SWAPP.

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

Table 4 Threats

3.2. Assumptions

The following assumptions are drawn directly from the SWAPP.

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

Table 5 Assumptions

3.3. Organizational Security Policies

There are no OSPs for the application

4. Security Objectives

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

4.1. Security Objectives for the TOE

The following security objectives for the TOE were drawn directly from the SWAPP.

ID	TOE Objective
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom if ever shipped without errors, and the ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options. Addressed by: FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs. Addressed by: FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII. Addressed by: FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1.5, FPR_ANO_EXT.1
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data. Addressed by: FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application. Addressed by: FTP_DIT_EXT.1, FCS_TLSC_EXT.1, FCS_DTLS_EXT.1, FCS_RBG_EXT.1

Table 6 Objectives for the TOE

4.2. Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

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

Table 7 Objectives for the environment

5. Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 or Common Criteria for Information Technology Security Evaluations, Version 3.1, Revision 4 extended and all international interpretations.

Requirement	Auditable Event
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.4	TLS Client Protocol
FDP_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

Table 8 SFRs

5.1. Conventions

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

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

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

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

5.2. Security Functional requirements

5.2.1. Cryptographic Support (FCS)

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1

The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_ HTTPS _EXT.1.2

The application shall implement HTTPS using TLS in accordance with [FCS_TLSC_EXT.1].

FCS_ HTTPS _EXT.1.3

The application shall [notify the user and not establish the connection] if the peer certificate is deemed invalid.

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [use no DRBG functionality] for its cryptographic operations

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [not store any credentials] to non-volatile memory.

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1

The application shall [invoke platform-provided TLS 1.2] supporting the following cipher suites:

[

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FCS_TLSC_EXT.1.2

The application shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3

The application shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.4 TLS Client Protocol

FCS_TLSC_EXT.4.1

The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1].

5.2.2. User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [network connectivity, camera, and location services].

FDP_DEC_EXT.1.2

The application shall restrict its access to [address book].

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [user-initiated communication for *[updating contacts]*].

FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [leverage platform-provided functionality to encrypt sensitive data] in non-volatile memory.

5.2.3. Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1

The application shall [invoked platform-provided functionality] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints

extension and that the CA flag is set to TRUE for all CA certificates.

- The application shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560].
- The application shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kpcmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

FIA_X509_EXT.1.2

The application shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1

The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS].

FIA_X509_EXT.2.2

When the application cannot establish a connection to determine the validity of a certificate, the application shall [not accept the certificate].

5.2.4. Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

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

FMT_CFG_EXT.1.2

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

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [no management functions].

5.2.5. Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1

The application shall [not transmit PII over a network].

5.2.6. Protection of TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall only use documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

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

FPT_AEX_EXT.1.2

The application shall [not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3

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

FPT_AEX_EXT.1.4

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

FPT_AEX_EXT.1.5

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

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

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

FPT_TUD_EXT.1.2

The application shall be distributed using the format of the platform supported package manager.

FPT_TUD_EXT.1.3

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.1.4

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

FPT_TUD_EXT.1.5

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

FPT_TUD_EXT.1.6

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

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1

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

5.2.7. Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [encrypt all transmitted data with [HTTPS, TLS]] between itself and another trusted IT product.

5.3. TOE SFR Dependencies Rationale for SFRs

The Protection Profile for Application Software contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.4. Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Protection Profile for Application Software which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic Functional Specification

Assurance Class	Components	Components Description
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
	ALC_TSU_EXT.1	Timely Security Updates
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

Table 9 Security Assurance Requirements

5.5. Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6. Assurance Measures

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

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.

SAR Component	How the SAR will be met
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ALC_TSU_EXT.1	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.
ATE_IND.1	Apple will provide the TOE for testing.
AVA_VAN.1	Apple will provide the TOE for testing.

Table 10 TOE Security Assurance Measures

6. TOE Summary Specification

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

TOE SFR	Rationale
FCS_HTTPS_EXT.1	The TOE implements RFC 2818 and leverages TLS 1.2 for establishing a secure connection.
FCS_RBG_EXT.1	The TOE does not use DRBG functionality for its cryptographic operations Due to leveraging of platform cryptographic functionality there are no TOE functions covered by ST SFRs that use random numbers provided by the platform. All random numbers used by SFR related functions are used by the platform's underlying cryptographic functionality.
FCS_STO_EXT.1	The contacts application does not store any credentials. Each contact is stored on the platform for use by the application is stored under Class C (Protected Until First User Authentication- NSFileProtectionComplete). However, no, credentials are stored.
FCS_TLSC_EXT.1 FCS_TLSC_EXT.4	The TOE leverages the platform implementation of TLS 1.2 in establishing secure connections to external IT entities (Apple Servers when sharing information at the user request). By default, TLS 1.0, TLS 1.1, SSL 2.0 and SSL 3.0 connections are denied. The TOE supports the following encryption algorithms for use with TLS connections: • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 During establishment of the TLS 1.2 session, the TOE platform will perform verification of the presented identifier in the peer certificate to ensure that it is a valid reference identifier. This ensures that the reference identifier is conformant with RFC 6125. 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. The TOE supports IP address and wildcards (via the TOE platform). Certificate pinning is not supported. The TOE, when acting as a client, provides responses to the server with a list of its supported curves, including, secp256r1 and secp384r1. These elliptic curves are supported by default and no configuration is required.
FDP_DAR_EXT.1	During operation of the TOE, any sensitive information stored securely is protected by platform-provided functionality to encrypt the sensitive data. 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.

TOE SFR	Rationale
FDP_DEC_EXT.1	The TOE requests only access to the following components: • Network connectivity • Camera • Location services • Address book
FDP_NET_EXT.1	The TOE communicates on the network based upon user-initiated actions.
FIA_X509_EXT.1	The TOE leverages X.509 certificate validation services provided by the TOE platform to validate certificates presented by its TLS connections. The X.509 certificates are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows: • the public key algorithm and parameters are checked • the current date/time is checked against the validity period • revocation status is checked • issuer name of X matches the subject name of X+1 • name constraints are checked • policy OIDs are checked • policy constraints are checked; issuers are ensured to have CA signing bits • path length is checked • critical extensions are processed In order to verify the revocation status of the presented certificates Online Certificate Status Protocol (OCSP) is used. Certificate processing is completely provided by the TOE platform.
FIA_X509_EXT.2	X.509v3 certificates are supported for authentication for TLS client connections. The TOE will only use the pre-installed certificates for TLS client connections. The TOE leverages "Trusted" digital certificates that pre-installed in the iOS Trust Store. The TOE will not leverage any other certificates for connections. 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. If the certificate is deemed to be invalid via a revocation check, the communication will cease immediately and a connection will not be established.
FMT_CFG_EXT.1	The TOE does not come with any default credentials. The user must configure an account first before accessing the TOE and underlying platform.
FMT_MEC_EXT.1	The TOE maintains a restricted configuration with no management functions being performed by users. All configuration options are stored and set by the underlying platform.
FMT_SMF.1	The TOE provides no management functionality.
FPR_ANO_EXT.1	The TOE does not request any PII with the intent to transmit the data over the network. However, the TOE will transmit contact information at the request of the user. In these cases, the TOE provides a notification when sharing this information. Note: this SFR only applies to PII that is specifically requested by the application.

TOE SFR	Rationale
FPT_AEX_EXT.1	The TOE is compiled with ASLR enabled (achieved by compiling with the -fPIE flag) and does not make any calls to mmap or mprotect. Stack-based buffer overflow protection is provided by being compiled with the -fstack-protector-all flag.
FPT_API_EXT.1	The following API frameworks are used by contacts: • Accounts.framework • AddressBook.framework • AppKit.framework • AppSupport.framework • AssistantServices.framework • Contacts.framework • ContactsDonation.framework • CoreData.framework • CoreFoundation.framework • CoreGraphics.framework • CoreSpotlight.framework • CoreSuggestions.framework • CoreText.framework • DataAccessExpress.framework • Foundation.framework • IntlPreferences.framework • PhoneNumber.framework • Security.framework • TCC.framework
FPT_LIB_EXT.1	The TOE does not leverage any third-party libraries. It is a 1st part application that is provided on the underlying platform by the vendor.
FPT_TUD_EXT.1	The TOE is provided within the underlying OS image and packaged as a signed IPA file. iOS considers the signature authorized if the certificate used to sign the IPA file chains to the Apple Worldwide Developer Relations Certification Authority or the Apple iPhone Certification Authority. Updates to the TOE are provided through the App Store and current versions of the TOE can be checked through the Settings of the underlying platform.
FTP_DIT_EXT.1	All application data is transmitted securely via HTTPS and TLS with Apple Servers.

Table 11 TOE Summary Specification SFR Description