Apple iOS 14 and iPadOS 14: Contacts Security Target

Document Version: 1.2
Date: August 2021

Prepared for:
Apple
One Apple Park Way
Cupertino, CA 95014

Prepared by:


2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History:

Version	Date	Changes
1.0	July 2021	Initial Release
1.1	August 2021	Updated to address ECR comments
1.2	August 2021	Minor updates

Trademarks

Apple's trademarks applicable to this document are listed in
https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html

Other company, product, and service names may be trademarks or service marks of others.

Contents

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

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

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Apple iOS 14 and iPadOS 14: Contacts Security Target
ST Version	1.2
ST Date	August 2021
ST Author	Acumen Security, LLC
TOE Identifier	Apple iOS 14 and iPadOS 14: Contacts
TOE Version	14.2
TOE Developer	Apple Inc.
Key Words	Application, Mobility

1.2 TOE Overview

The TOE is the Apple Contacts application running on Apple iOS 14 and iPadOS 14. Contacts allows a user to access and edit contacts from personal, business, and other accounts.

Contacts is a first-party app, distributed with the operating system of the iPhone and iPad devices. Users can add contacts manually and/or they can be synchronized with an external server.

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

1.3 TOE Description

This section provides a general description of the TOE, including physical boundaries, security functions, and relevant TOE documentation and references.

1.3.1 Physical Boundaries

The TOE does not have a physical boundary because the TOE is a software application. As evaluated, the TOE runs on the following physical devices:

Table 2 – Hardware Platforms

Device Name	Model	OS	Processor
iPhone 12 Pro Max	A2342 A2410 A2411 A2412	iOS	Apple A14 Bionic
iPhone 12 Pro	A2341 A2406 A2407 A2408	iOS	Apple A14 Bionic

Device Name	Model	OS	Processor
iPhone 12	A2172 A2402 A2403 A2404	iOS	Apple A14 Bionic
iPhone 12 mini	A2176 A2398 A2399 A2400	iOS	Apple A14 Bionic
iPhone 11 Pro Max	A2161 A2218 A2219 A2220	iOS	Apple A13 Bionic
iPhone 11 Pro	A2160 A2215 A2217	iOS	Apple A13 Bionic
iPhone 11	A2111 A2221 A2223	iOS	Apple A13 Bionic
iPhone SE (2nd generation)	A2275 A2296 A2298	iOS	Apple A13 Bionic
iPhone Xs Max	A1921 A2101 A2102 A2104	iOS	Apple A12 Bionic
iPhone Xs	A1920 A2097 A2098 A2099 A2100	iOS	Apple A12 Bionic
iPhone Xr	A1984 A2105 A2106 A2107 A2108	iOS	Apple A12 Bionic
iPhone X	A1865 A1901 A1902	iOS	Apple A11 Bionic
iPhone 8 Plus	A1864 A1897 A1898 A1899	iOS	Apple A11 Bionic
iPhone 8	A1863 A1905 A1906 A1907	iOS	Apple A11 Bionic
iPhone 7 Plus	A1661 A1784 A1785 A1786	iOS	Apple A10 Fusion

Device Name	Model	OS	Processor
iPhone 7	A1660 A1778 A1779 A1780	iOS	Apple A10 Fusion
iPhone 6s Plus	A1634 A1687 A1690 A1699	iOS	Apple A9
iPhone 6s	A1633 A1688 A1691 A1700	iOS	Apple A9
iPhone SE	A1662 A1723 A1724	iOS	Apple A9
iPad Air (4th generation)	A2316 A2324 A2072 A2325	iPadOS	Apple A14 Bionic
iPad Pro 12.9-inch (4th generation)	A2229 A2232 A2069 A2233	iPadOS	Apple A12Z Bionic
iPad Pro 11-inch (2nd generation)	A2228 A2068 A2230 A2331	iPadOS	Apple A12Z Bionic
iPad Pro 12.9-inch (3rd generation)	A1876 A1895 A1983 A2014	iPadOS	Apple A12X Bionic
iPad Pro 11-inch (1st generation)	A1980 A1934 A1979 A2013	iPadOS	Apple A12X Bionic
iPad (8th generation)	A2270 A2428 A2429 A2430	iPadOS	Apple A12 Bionic
iPad Air (3rd generation)	A2123 A2152 A2153 A2154	iPadOS	Apple A12 Bionic
iPad mini (5th generation)	A2124 A2125 A2126 A2133	iPadOS	Apple A12 Bionic
iPad Pro (12.9-inch) (2nd generation)	A1670 A1671 A1821	iPadOS	Apple A10X Fusion

Device Name	Model	OS	Processor
iPad Pro (10.5-inch)	A1701 A1709 A1852	iPadOS	Apple A10X Fusion
iPad (7th generation)	A2198 A2199 A2200	iPadOS	Apple A10 Fusion
iPad (6th generation)	A1893 A1954	iPadOS	Apple A10 Fusion
iPad Pro (12.9-inch)	A1584 A1652	iPadOS	Apple A9X
iPad Pro (9.7-inch)	A1673 A1674 A1675	iPadOS	Apple A9X
iPad (5th generation)	A1822 A1823	iPadOS	Apple A9

1.3.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Protection Profile for Application Software Version 1.3 (PP_APP_v1.3).

1.3.2.1 Cryptographic Support

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

1.3.2.2 User Data Protection

The TOE utilizes network and address book access. The TOE requests camera and photos library access to associate pictures with contacts.

1.3.2.3 Identification and Authentication

The TOE uses platform-provided X.509 certificate validation functions to verify the validity and revocation status of HTTPS/TLS server certificates.

1.3.2.4 Security Management

The TOE does not provide management functionality. All management of settings is performed by the underlying platform. The TOE reads the platform-configured settings.

1.3.2.5 Privacy

The TOE does not request any personally identifiable information (PII) with the intent to transmit the data over the network. However, the TOE will transmit contact information at the request of the user.

1.3.2.6 Protection of the TSF

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

1.3.2.7 Trusted Path/Channels

The TOE is a software application. The TOE has the ability to establish protected communications using platform-provided TLS/HTTPS.

1.3.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- [ST] Apple iOS 14 and iPadOS 14: Contacts Security Target, Version 1.2 (This Document)
- [AGD] Apple iOS 14 and iPadOS 14: Contacts Common Criteria Configuration Guide, Version 1.2

1.4 TOE Environment

The following environmental components interoperate with the TOE in the evaluated configuration:

Table 3 – Environmental Components

Component	Description
Hardware Platform	See Table 2
Operating System	Apple iOS 14.2 or Apple iPadOS 14.2
Remote Server (optional)	Server for storing and synchronizing contacts

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017

The TOE and ST are Part 2 extended and Part 3 extended.

2.2 Protection Profile Conformance

This ST claims exact conformance to the Protection Profile for Application Software, Version 1.3, March 1, 2019.

2.3 Conformance Rationale

This ST provides exact conformance to PP_APP_v1.3. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to PP_APP_v1.3 have been considered. Table 4 identifies all applicable TDs.

Table 4 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0416: Correction to FCS_RBG_EXT.1 Test Activity	Yes	
TD0427: Reliable Time Source	Yes	
TD0434: Windows Desktop Applications Test	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
TD0437: Supported Configuration Mechanism	Yes	
TD0445: User Modifiable File Definition	Yes	
TD0465: Configuration Storage for .NET Apps	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0473: Support for Client or Server TOEs in FCS_HTTPS_EXT	No	The TOE uses platform-provided HTTPS, so it does not include FCS_HTTPS_EXT.1.
TD0495: FIA_X509_EXT.1.2 Test Clarification	No	The TOE does not directly invoke X.509 functionality.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0498: Application Software PP Security Objectives and Requirements Rationale	Yes	
TD0510: Obtaining random bytes for iOS/macOS	No	The TOE does not obtain random bytes from the platform.
TD0515: Use Android APK manifest in test	No	This TD only applies to Android platforms. The TOE runs on iOS and iPadOS.
TD0519: Linux symbolic links and FMT_CFG_EXT.1	No	This TD only applies to Linux platforms. The TOE runs on iOS and iPadOS.
TD0540: Expanded AES Modes in FCS_COP	No	The TOE does not implement AES.
TD0543: FMT_MEC_EXT.1 evaluation activity update	No	This TD only applies to Windows platforms. The TOE runs on iOS and iPadOS.
TD0544: Alternative testing methods for FPT_AEX_EXT.1.1	Yes	
TD0548: Integrity for installation test in AppSW PP 1.3	Yes	
TD0554: iOS/iPadOS/Android AppSW Virus Scan	Yes	
TD0561: Signature verification update	Yes	
TD0582: PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed	Yes	
TD0587: X.509 SFR Applicability in App PP	Yes	

3 Security Problem Definition

The security problem definition is taken directly from the claimed PP specified in Section 2.2 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 (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 5 are drawn directly from the PP specified in Section 2.2.

Table 5 – Threats

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.

3.2 Assumptions

The assumptions included in Table 6 are drawn directly from the PP.

Table 6 – Assumptions

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock 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 in compliance with the applied enterprise security policy.

3.3 Organizational Security Policies

The PP does not define any OSPs.

4 Security Objectives

The security objectives have been taken directly from the claimed PP and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The security objectives in the following table apply to the TOE.

Table 7 – Security Objectives

ID	Security Objectives
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. 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.
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.
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.
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 in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
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.

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 8 – Security Objectives for the Operational Environment

ID	Objectives for the Operational 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.

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, September 2017, and all international interpretations.

Table 9 – SFRs

Requirement	Description
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
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 Information
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_IDV_EXT.1	Software Identification and Versions
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

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the PP, the formatting has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Cryptographic Support (FCS)

5.2.1.1 FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1
The application shall [

- *generate no asymmetric cryptographic keys,*

].

5.2.1.2 FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1
The application shall [

- *use no DRBG functionality*,

] for its cryptographic operations.

5.2.1.3 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1
The application shall [

- *not store any credentials*,

] to non-volatile memory.

5.2.2 User Data Protection (FDP)

5.2.2.1 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.

5.2.2.2 FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1
The application shall restrict its access to [

- *network connectivity*,
- *camera*,

].

FDP_DEC_EXT.1.2
The application shall restrict its access to [

- *address book*,
- *[photos library]*

].

5.2.2.3 FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1
The application shall restrict network communication to [

- *user-initiated communication for [updating contacts],*

].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_X509.EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1
The application shall [invoke 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, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [an OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066]
- The application shall validate the extendedKeyUsage (EKU) 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 EKU 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 EKU 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 EKU 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 EKU field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

Application Note: This SFR has been updated by TD0587.

FIA_X509_EXT.1.2
The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.2 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*].

Application Note: This SFR has been updated by TD0587.

FIA_X509_EXT.2.2
When the application cannot establish a connection to determine the validity of a certificate, the application shall [*accept the certificate*].

5.2.4 Security Management (FMT)

5.2.4.1 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1
The application shall provide only 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 binaries and data files from modification by normal unprivileged users.

5.2.4.2 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.].

5.2.4.3 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)

5.2.5.1 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1
The application shall [

- *not transmit PII over a network ,*

].

5.2.6 Protection of the TSF (FPT)

5.2.6.1 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 [no exceptions].

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 built with stack-based buffer overflow protection enabled.

5.2.6.2 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1
The application shall use only documented platform APIs.

5.2.6.3 FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1
The application shall be versioned with [*[Bundle configuration information (Name, Bundle ID and version)]*] .

5.2.6.4 FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1
The application shall be packaged with only [no third-party libraries].

5.2.6.5 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 [*leverage the platform*] to query the current version of the application software.

FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5
The application is distributed [*with the platform OS*]

5.2.7 Trusted Path/Channel (FTP)

5.2.7.1 FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1
The application shall [

- *invoke platform-provided functionality to encrypt all transmitted data with [HTTPS, TLS]*

] between itself and another trusted IT product.

Application Note: This SFR has been updated by TD0587.

5.3 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 10.

Table 10 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling 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

5.4 Assurance Measures

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

Table 11 – TOE Security Assurance Measures

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.
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	This component requires the TOE developer, in conjunction with any other necessary parties, to provide information as to how the end-user devices are updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, carriers(s)) and the steps that are performed (e.g., developer testing, carrier testing), including worst case time periods, before an update is made available to the public.
ATE_IND.1	Apple will provide the TOE for testing.
AVA_VAN.1	Apple will provide the TOE for testing. FPT_LIB_EXT.1 identifies the list of third-party software components.

6 TOE Summary Specification

This chapter identifies and describes how the SFRs identified above are met by the TOE.

Table 12 – TOE Summary Specification SFR Description

Requirement	TSS Description
ALC_TSU_EXT.1	Apple generally does not disclose, discuss, or confirm security issues until a full investigation is complete and any necessary patches or releases are available. Once an issue has been confirmed and a patch has been made available, references containing technical details on the patches are made available and Common Vulnerabilities and Exposures (CVEs), etc. are released. Apple distributes information about security issues in its products through its "Apple security updates" page. (https://support.apple.com/HT201222) Security advisories are also provided through the security-announce mailing list. (https://lists.apple.com/mailman/listinfo/security-announce/) Potential security vulnerabilities can be reported by following the procedures on the "Report a security or privacy vulnerability" page (https://support.apple.com/HT201220). This includes sending an email to "product-security@apple.com" and includes the ability to encrypt information using the Apple Product Security PGP key. (https://support.apple.com/kb/HT201214)
FCS_CKM_EXT.1	The TOE does not perform asymmetric key generation.
FCS_RBG_EXT.1	The TOE does not use DRBG functionality.
FCS_STO_EXT.1	The TOE does not store any credentials. Credentials used for user-initiated updates of contact data are stored by the platform. These credentials are used (along with platform-provided TLS/HTTPS) by the platform when the user initiates an update.
FDP_DAR_EXT.1	Contact data is the only data and the only sensitive data stored by the TOE. The TOE securely stores sensitive data using platform-provided functionality to encrypt the data, specifically stored under Class C: Protected Until First User Authentication (NSFileProtectionCompleteUntilFirstUserAuthentication).
FDP_DEC_EXT.1	The TOE requests access to the following hardware resources: • Network connectivity – synchronizing contacts • Camera – associating pictures with contacts The TOE limits its access to the following sensitive information repository: • Address Book database – updating the local database of contacts • Photos Library – associating pictures with contacts
FDP_NET_EXT.1	The TOE communicates on the network based upon user-initiated request to update contacts. Note: The platform can also be configured to periodically update the platform Address Book database independently of the Contacts application.
FIA_X509_EXT.1 FIA_X509_EXT.2	The TOE invokes platform-provided X.509 certificate validation to verify the validity and revocation status of HTTPS/TLS server

Requirement	TSS Description
	certificates. The platform-provided functionality validates certificates according to the following rules: • RFC 5280 certificate validation and certificate path validation. • The certificate path must terminate with a trusted CA certificate marked as a trust anchor in the platform's Certificate Trust Settings. • All CA certificates contain the basicConstraints extension with the CA flag is set to TRUE and (if present) path constraints are met. • All CA certificates include the caSigning bit in the key usage field. • Certificate revocation status is checked using OCSP stapling. The Certificate Status Request extension is sent in the Client Hello. The OCSP response is contained in the Certificate Status message sent by the server. The certificate is accepted if its revocation status cannot be determined. The extendedKeyUsage field for TLS server certificates is verified to contain the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1). The extendedKeyUsage field for OCSP signing certificates is verified to contain the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9. X.509 certificates are validated during session establishment with an HTTPS/TLS server. The platform uses the certificates provided by the TLS server and the certificates in the local trust store to build the certificate chain.
FMT_CFG_EXT.1	The TOE does not come with any default credentials. The user must configure an account on the underlying platform to enable synchronization of contacts with a remote server.
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. The TOE reads configuration options from the platform's user defaults system.
FMT_SMF.1	The TOE does not provide management functionality. All management of settings is performed by the underlying platform.
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.
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. The TOE does not allocate any memory regions with the PROT_EXEC permission.

Requirement	TSS Description
	The underlying platform is iOS or iPadOS, so the platform ensures the TOE: 1) Is compatible with the platform security features, 2) Writes data to the application working directory and not the directory containing executable files. The TOE is compiled with stack-based buffer overflow protection enabled (achieved by compiling with the -fstack-protector-all flag).
FPT_API_EXT.1	The following API frameworks are used by the TOE: • 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_IDV_EXT.1	Each iOS and iPadOS application is distributed 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: 14.2
FPT_LIB_EXT.1	The TOE does not leverage any third-party libraries. It is a first-party 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. The platform 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 the current version of the TOE can be checked through the Settings app of the underlying platform.
FTP_DIT_EXT.1	All application data is transmitted securely via platform-provided HTTPS and TLS with Apple servers or other configured servers.

Requirement	TSS Description
	The TOE uses the NSURL class to initiate a synchronization of contacts with the servers. User credentials are transmitted during the synchronization process; however, credentials are managed and transmitted by the platform OS as necessary.

7 Acronyms

Table 13 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AppSW	Application Software Protection Profile
ASLR	Address Space Layout Randomization
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CVE	Common Vulnerabilities and Exposures
DRBG	Deterministic Random Bit Generator
EKU	Extended Key Usage
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
NIAP	Nation Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
RFC	Request for Comments
RSA	Rivest, Shamir, & Adleman
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TD	Technical Decision
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification
VID	Validation Identifier
VPN	Virtual Private Network