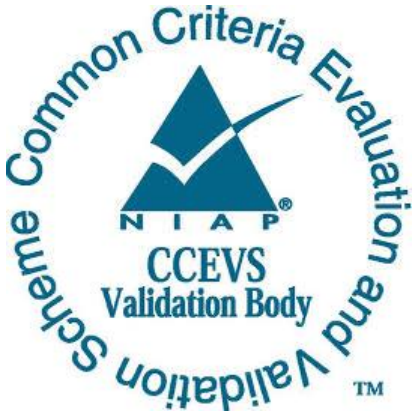
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Apple iOS 16: iPhones

Report Number: **CCEVS-VR-VID11349-2023**
Dated: **October 10, 2023**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick W. Mallett, Ph.D.
Jerome F. Myers, Ph.D.
Seada Mohammed
VietHung D Le
The Aerospace Corporation

Common Criteria Testing Laboratory

Trang Huynh
King Ables
Travis Hoffmeister
Walker Riley
Joachim Vandersmissen
Joanna Labastida
Stephan Mueller
atsec information security corporation, Austin TX

Table of Contents

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Apple iOS 16: iPhones provided by Apple Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in October 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Extended and meets the assurance requirements given in:

- PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0 (CFG_MDF-BIO-BT-MDMA-VPNC-WLANC_V1.0)

  This PP-Configuration is comprised of the following components:

  - Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3 (PP_MDF_V3.3)
  - PP-Module: collaborative PP-Module for Biometric enrolment and verification – _for unlocking the device – _[BIOPP-Module], Version 1.1 (MOD_CPP_BIO_V1.1)
  - PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0)
  - PP-Module for MDM Agents, Version 1.0 (MOD_MDM_AGENT_V1.0)
  - PP-Module for Virtual Private Network (VPN) Clients, Version 2.4 (MOD_VPNC_V2.4)
  - PP-Module for WLAN Clients, Version 1.0 (MOD_WLANC_V1.0)
- Package
  - Functional Package for Transport Layer Security (TLS), Version 1.1 (PKG_TLS_V1.1)

The TOE is Apple iOS 16: iPhones executing on the following platforms:

- iPhone 8/iPhone 8 Plus (A11 Bionic processor)
- iPhone X (A11 Bionic processor)
- iPhone XS/iPhone XS Max (A12 Bionic processor)
- iPhone XR (A12 Bionic processor)

- iPhone 11/iPhone 11 Pro/iPhone 11 Pro Max (A13 Bionic processor)
- iPhone SE (2nd gen) (A13 Bionic processor)
- iPhone 12 mini/iPhone 12/iPhone 12 Pro/iPhone 12 Pro Max (A14 Bionic processor)
- iPhone 13 mini/iPhone 13/iPhone 13 Pro/iPhone 13 Pro Max (A15 Bionic processor)
- iPhone SE (3rd gen) (A15 Bionic processor)
- iPhone 14/iPhone 14 Plus (A15 Bionic processor)
- iPhone 14 Pro/iPhone 14 Pro Max (A16 Bionic processor)

The TOE identified in this Validation Report has been evaluated at a NIAP-approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC) and the Assurance Activities (AA) of the aforementioned PP-Configuration, Protection Profile, PP Modules, and Extended Packages. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, reviewed testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The atsec information security corporation CCTL evaluation team concluded that the CC requirements specified by:

- PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0

  This PP-Configuration is comprised of the following components:

  - Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3 (PP_MDF_V3.3)
  - PP-Module: collaborative PP-Module for Biometric enrolment and verification – _for unlocking the device – _[BIOPP-Module], Version 1.1 (MOD_CPP_BIO_V1.1)
  - PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0)
  - PP-Module for MDM Agents, Version 1.0 (MOD_MDM_AGENT_V1.0)

    - PP-Module for Virtual Private Network (VPN) Clients, Version 2.4 (MOD_VPNC_V2.4)
    - PP-Module for WLAN Clients, Version 1.0 (MOD_WLANC_V1.0)
- Functional Package for Transport Layer Security (TLS), Version 1.1

have been met.

The technical information included in this report was obtained from the Apple iOS 16: iPhones Security Target, Version 1.0.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

The following table provides information needed to completely identify the product, including the following.

- The Target of Evaluation (TOE): The fully qualified identifier of the product as evaluated
- The ST: Describing the security features, claims, and assurances of the product
- The conformance results of the evaluation
- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iOS 16: iPhones executing on the following platforms: • iPhone 8/iPhone 8 Plus (A11 Bionic processor) • iPhone X (A11 Bionic processor) • iPhone XS/iPhone XS Max (A12 Bionic processor) • iPhone XR (A12 Bionic processor) • iPhone 11/iPhone 11 Pro/iPhone 11 Pro Max (A13 Bionic processor) • iPhone SE (2nd gen) (A13 Bionic processor) • iPhone 12 mini/iPhone 12/iPhone 12 Pro/iPhone 12 Pro Max (A14 Bionic processor) • iPhone 13 mini/iPhone 13/iPhone 13 Pro/iPhone 13 Pro Max (A15 Bionic processor) • iPhone SE (3rd gen) (A15 Bionic processor) • iPhone 14/iPhone 14 Plus (A15 Bionic processor) • iPhone 14 Pro/iPhone 14 Pro Max (A16 Bionic processor)
PP	• PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0 This PP-Configuration is comprised of the following components: o Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3 o PP-Module: collaborative PP-Module for Biometric enrolment and verification – _for unlocking the device – _[BIOPP-Module], Version 1.1 o PP-Module for Bluetooth, Version 1.0 o PP-Module for MDM Agents, Version 1.0 o PP-Module for Virtual Private Network (VPN) Clients, Version 2.4 o PP-Module for WLAN Clients, Version 1.0 Functional Package for Transport Layer Security (TLS), Version 1.1
ST	Apple iOS 16: iPhones Security Target (ST), Version 1.1, dated 2023-09-26
ETR	Evaluation Technical Report for a Target of Evaluation Apple iOS 16: iPhones, Version 1.0, dated 2023-09-19
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended

Item	Identifier
Sponsor	Apple Inc.
Developer	Apple Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Patrick W. Mallett, Jerome F. Myers, Seada Mohammed, VietHung D Le

3. Architectural Information

Note that the following architectural description is based on the description presented in the ST.

The implementation of TOE architecture can be viewed as a set of layers. Lower layers contain fundamental services and technologies. Higher-level layers build upon the lower layers and provide more sophisticated services and technologies.

These individual layers provide the following services.

The **Cocoa Touch layer** contains key frameworks for building apps. These frameworks define the appearance of apps. They also provide the basic app infrastructure and support for key technologies such as multitasking, touch-based input, push notifications, and many high-level system services.

The **Media layer** contains the graphics, audio, and video technologies you use to implement multimedia experiences in apps.

The **Core Services layer** contains fundamental system services for apps. Key among these services are the Core Foundation and Foundation frameworks, which define the basic types that all apps use. This layer also contains individual technologies to support features such as location, iCloud, social media, and networking.

This layer also implements data protection functions that allow apps that work with sensitive user data to take advantage of the built-in encryption available on some devices. When an app designates a specific file as protected, the system stores that file in an encrypted format. While the device is locked, the contents of the file are inaccessible to both the app and to any potential intruders. However, when the device is unlocked by the user, a decryption key is created to allow the app to access the file. Other levels of data protection are also available.

The **Core OS layer** contains the low-level features that most other technologies are built upon. Even if an app does not use these technologies directly, they are most likely being used by other frameworks. And in situations where an app needs to explicitly deal with security or communicating with an external hardware accessory, it does so by using the frameworks in this layer.

Security-related frameworks provided by this layer are as follows:

- the Generic Security Services Framework, providing services as specified in Request for Comment (RFC) 2743 (Generic Security Service Application Program Interface Version 2, Update 1) and RFC 4401 (Pseudo Random Function);

- the Local Authentication Framework;
- the Network Extension Framework, providing support for configuring and controlling VPN tunnels;
- the Security Framework, providing services to manage and store certificates, public and private keys, and trust policies (this framework also provides the Common Crypto library for symmetric encryption and hash-based message authentication codes); and
- the System Framework, providing the kernel environment, drivers, and low-level UNIX interfaces (the kernel manages the virtual memory system, threads, file system, network, and inter-process communication and is therefore responsible for separating apps from each other and controlling the use of low-level resources).

The TOE is managed by an MDM solution that enables an enterprise to control and administer the TOE instances that are enrolled in the MDM solution.

TOE Evaluated Configuration

The evaluated configuration consists of the following hardware and software, when configured in accordance with the documentation specified in Section 6. The evaluation covers the following Apple iPhones running iOS 16 operating system as detailed in Table 1.

Table 1: Devices covered by the evaluation

Processor	Device Name	Model Number
A11 Bionic	iPhone 8	A1863
		A1906
		A1907
		A1905
	iPhone 8 Plus	A1864
		A1898
		A1899
		A1897
	iPhone X	A1865
		A1902
		A1901
A12 Bionic	iPhone XS	A1920
		A2097
		A2098

Processor	Device Name	Model Number
		A2099
		A2100
	iPhone XS Max	A1921
		A2101
		A2102
		A2104
	iPhone XR	A1984
		A2105
		A2106
		A2107
		A2108
A13 Bionic	iPhone 11	A2111
		A2221
		A2223
	iPhone 11 Pro	A2160
		A2215
		A2217
	iPhone 11 Pro Max	A2161
		A2218
		A2220
	iPhone SE (2nd gen)	A2275
		A2296
		A2298
A14 Bionic	iPhone 12 mini	A2176
		A2398
		A2399
		A2400
	iPhone 12	A2172
		A2402

Processor	Device Name	Model Number
		A2403
		A2404
	iPhone 12 Pro	A2341
		A2406
		A2407
		A2408
	iPhone 12 Pro Max	A2342
		A2410
		A2411
		A2412
A15 Bionic	iPhone 13 mini	A2481
		A2626
		A2628
		A2629
		A2630
	iPhone 13	A2482
		A2631
		A2633
		A2634
		A2635
	iPhone 13 Pro	A2483
		A2636
		A2638
		A2639
		A2640
	iPhone 13 Pro Max	A2484
		A2641
		A2643
		A2644
		A2645
	iPhone SE (3rd gen)	A2595
		A2782
		A2783
		A2785
	iPhone 14	A2649
		A2881

Processor	Device Name	Model Number
A16 Bionic		A2882
		A2883
		A2884
	iPhone 14 Plus	A2632
		A2885
		A2886
		A2887
		A2888
	iPhone 14 Pro	A2650
		A2889
		A2890
		A2891
		A2892
	iPhone 14 Pro Max	A2651
		A2893
		A2894
		A2895
		A2896

Physical Scope of the TOE

The TOE is a Mobile Device that consists of a hardware platform and its system software. It provides wireless connectivity and includes software for VPN connections to access the protected enterprise network and other Mobile Devices.

The TOE provides secured communication channels between itself and other trusted IT products using IEEE 802.11-2012, IEEE 802.11ac-2013 (a.k.a. Wi-Fi 5), IEEE 802.11ax (a.k.a. Wi-Fi 6), IEEE 802.1X, EAP-TLS (v1.1, v1.2), TLS (v1.2), IPsec and Bluetooth (v5.0, v5.3). Via the established network connection, the TOE can communicate with an MDM server allowing administrative control of the TOE.

Un-evaluated Functionality

The following functions were not evaluated and are, therefore, not included in the secure configuration of the Mobile Devices.

- **Two-Factor Authentication**

  Two-factor authentication is an extra layer of security for an Apple ID used in the Apple store, iCloud, and other Apple services.

- **Bonjour**

  Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network.

- **VPN Split Tunnel**

  VPN split tunnel is not included in the evaluation and must be disabled in the Mobile Device configurations to meet the requirements of this CC evaluation.

- **Siri Interface**

  The Siri interface is capable of supporting commands related to configuration settings.

- **Third-party MDM Agents**

  Third-party applications are available that provide functionality as a Mobile Device MDM Agent. No third-party MDM Agent applications were included in the evaluation and are outside the scope of the evaluated configuration.

- **VPN Protocols and Authentication Methods**

  The following Virtual Private Network (VPN) protocols are not included in the evaluation and must be disabled in the Mobile Device configurations that meet the requirements of this CC evaluation.

  - Cisco IPsec
  - Layer Two Tunneling Protocol (L2TP) over IPsec
  - Secure Sockets Layer (SSL) VPN
  - Shared secret authentication

- **Face ID with a Mask**
  Face unlock with a face mask was not included in the evaluation. The Face ID with a Mask setting must be disabled in the evaluated configuration.

4. Security Policy

This section summaries the security functionality of the TOE including the following.

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Protection of the TSF (TOE Security Functionality)
7. TOE access
8. Trusted Path/Channels
9. Objective Requirements

Security Audit

The TOE provides the ability for responses to be sent from the MDM Device Agent to the MDM Server. These responses are configurable by the organization as per the Over-the-Air Profile Delivery and Configuration document.

Cryptographic Support

The TOE provides cryptographic services for the encryption of data at rest, secure communication channels, and for use by applications. In addition, the TOE implements several cryptographic protocols that can be used to establish a trusted channel to other IT entities.

The TOE provides cryptographic services via the following cryptographic modules.

- Apple corecrypto Module v13.0 [Apple ARM, User, Software, SL1]
- Apple corecrypto Module v13.0 [Apple ARM, Kernel, Software, SL1]
- Apple corecrypto Module v13.0 [Apple ARM, Secure Key Store, Hardware, SL2]

The **Apple corecrypto Module v13.0 [Apple ARM, User, Software, SL1]** is a dynamically loadable library that resides within the TOE OS user space. The library is loaded into an app running in user space to provide cryptographic functions.

The functions listed below are used to implement the security protocols supported and the encryption of data at rest.

- Random number generation
- Data encryption and decryption
- Signature generation/verification
- Message digest
- Message authentication
- Key derivation (PBKDF2)
- Key generation
- Key wrapping

The **Apple corecrypto Module v13.0 [Apple ARM, Kernel, Software, SL1]** is a TOE OS kernel extension (KEXT) optimized for library use within the TOE OS kernel. Once the module is loaded into the kernel, its cryptographic functions are made available to TOE OS Kernel services only.

The functions listed below are used to implement the security protocols supported as well as for the encryption of data at rest.

- Random number generation
- Data encryption/decryption

- Signature generation/verification
- Message digest
- Message authentication
- Key generation
- Key wrapping

The **Apple corecrypto Module v13.0 [Apple ARM, Secure Key Store, Hardware, SL2]** is a single-chip standalone hardware cryptographic module (System on a Chip (SoC)/System-in-Package (SiP)) running on a multi-chip device and provides services intended to protect data in transit and at rest. It contains both firmware and hardware cryptographic algorithm implementations. (The Secure Key Store is also known as the SKS.)

The cryptographic services provided by the module are:

- Random number generation
- Data encryption/decryption
- Message digest
- Message authentication
- Key generation
- Key wrapping

User Data Protection

User data in files is protected using cryptographic functions, ensuring this data remains protected even if the device gets lost or is stolen. Critical data (like passcodes used by apps or application-defined cryptographic keys) can be stored in the key chain, which provides additional protection. Passcode protection and encryption ensure that data at rest remains protected even in the case of the device being lost or stolen.

The Secure Enclave Processor (SEP), a separate CPU that executes a stand-alone operating system and has separate memory, provides protection for critical security data such as keys.

Data is protected such that only the app that owns the data can access it.

Identification and Authentication

Except for making/answering calls, emergency calls, accessing Medical ID information, using the cameras (unless their use is generally disallowed), using the flashlight, using the control center, and using the notification center, users need to authenticate using a passcode or a biometric (fingerprint or face). The user is required to use the passcode authentication mechanism under the following conditions.

- Turn on or restart the device

- Press the Home button or swipe up to unlock your device (configurable)
- Update software
- Erase the device
- View or change passcode settings (including biometric enrollment)
- Install iOS Configuration Profiles

The passcode can be configured for a minimum length, for dedicated passcode policies, and for a maximum lifetime. When entered, passcodes are obscured and the frequency of entering passcodes is limited as well as the number of consecutive failed attempts of entering the passcode.

The TOE also enters a locked state after a (configurable) time of user inactivity and the user is required to either enter his passcode or use biometric authentication (fingerprint or face) to unlock the TOE.

The TOE's biometric face authentication is known as Face ID and its fingerprint authentication is known as Touch ID. There are also multiple generations of these BAFs.

External entities connecting to the TOE via a secure protocol (e.g., Transport Layer Security (TLS), Extensible Authentication Protocol Transport Layer Security (EAP-TLS), IPsec) can be authenticated using X.509 certificates.

Security Management

Security functions can be managed either by the user or by an authorized administrator through a Mobile Device Management system. Tables 15, 16, and 17 of the Security Target identify the functions that can be managed and if the management function can be performed by the user, the authorized administrator, or both.

Protection of the TSF

Some of the functions the TOE implements to protect the TSF and TSF data are as follows:

- Protection of cryptographic keys
- Use of memory protection and processor states to separate applications and protect the TSF from unauthorized access to TSF resources
- Digital signature protection of the TSF image
- Software/firmware integrity self-test upon startup
- Digital signature verification for apps
- Access to defined TSF data and TSF services only when the TOE is unlocked

TOE Access

The TSF provides functions to lock the TOE upon request and after an administrator-configurable time of inactivity.

Access to the TOE via a wireless network is controlled by user/administrator-defined policy.

Trusted Path/Channels

The TOE supports the use of the following cryptographic protocols that define a trusted channel between itself and another trusted IT product.

- IEEE 802.11-2012
- IEEE 802.11ac-2013 (a.k.a. Wi-Fi 5)
- IEEE 802.11ax (a.k.a. Wi-Fi 6)
- IEEE 802.1X
- EAP-TLS (v1.1, v1.2)
- TLS (1.2)
- IPsec
- Bluetooth (v5.0, v5.3)

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in the associated PP-Configuration:

- PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0

  This PP-Configuration is comprised of the following components:

  - Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3
  - PP-Module: collaborative PP-Module for Biometric enrolment and verification – _for unlocking the device – _[BIOPP-Module], Version 1.1
  - PP-Module for Bluetooth, Version 1.0
  - PP-Module for MDM Agents, Version 1.0
  - PP-Module for Virtual Private Network (VPN) Clients, Version 2.4
  - PP-Module for WLAN Clients, Version 1.0
- Functional Package for Transport Layer Security (TLS), Version 1.1

That information has not been reproduced here, and the respective documents should be consulted if there is interest in that material. Additionally, the Security Problem Description has been presented in the Security Target.

Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the ST and the associated PP-Configuration.

Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note: As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the PP_MDF_V3.3, MOD_CPP_BIOV1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0, and PKG_TLS_V1.1) performed by the evaluation team.

Specific exclusions from this evaluation are described in the subsection Un-evaluated Functionality in Section 3.

6. Documentation

The following documentation must be used to configure, administer, and use the product in its evaluated configuration.

Reference	Document Name	Location
[CCGUIDE]	Apple iOS 16: iPhones and Apple iPadOS 16: iPadsCommon Criteria Configuration Guide	https://www.niap-ccevs.org/MMO/Product/st_vid11349-agd.pdf https://www.niap-ccevs.org/MMO/Product/st_vid11350-agd.pdf

Any additional customer documentation that was not included in the scope of the evaluation should not be relied upon when configuring or using the products in the evaluated configuration.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. The specific test configurations and test tools utilized may be found in Section 2.3.4 of the Assurance Activity Report (AAR).

Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

Evaluation Team Independent Testing

The ST lists more devices compared to the subset of devices used for testing. The tests were performed on the Mobile Devices listed above, which were selected by choosing one from within each device family. The specific test configurations and test tools utilized may be found in the AAR.

One device family is defined by the hardware that impacts the TSF operation: the CPU. The other hardware, such as form factor, size of non-volatile storage, presence or absence of modem devices such as GSM, CDMA, or LTE do not affect the TSF. All TSF functions are solely implemented in software that uses the process isolation and memory separation capabilities offered by the CPU. The software of the TOE is compiled once to form one set of binaries, which run on all devices and, therefore, on all CPUs equally.

In addition, the security functions specified in the ST are all implemented above the hardware layer. Once a request is processed by the hardware, the security relevant decisions have been already made by the software. The hardware now only needs to enforce the functionality requested by the software. Based on this consideration, the evaluation team used the hardware information provided by the developer, which lists all devices found in the ST and references the CPUs used by those devices. All devices listed in the ST use one of the following CPUs:

- A11 Bionic
- A12 Bionic
- A13 Bionic
- A14 Bionic
- A15 Bionic
- A16 Bionic

The test system was set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing.

The basic testing infrastructure was configured as follows. The TOE is connected to a private WLAN network, which also hosts a Linux system as well as a macOS server.

The Linux server provides the following support:

- WLAN access point functionality
- Internet access
- network sniffer tools
- a VPN Gateway with the strongSwan IKE daemon and the Linux kernel IPsec support.

The macOS server provides the following support:

- MDM server
- Apple Configurator 2

The Linux system was equipped with the appropriate tools to perform sniffing of the different traffic types and analyzing the traffic, e.g., wireshark, tcpdump, and hcidump.

Apple Configurator 2 was used to create the configuration profiles/policies and deploy the profiles/policies onto the different test systems. An Apple system hosting the Apple Profile Manager software component acted as the MDM server to which the test devices connected.

8. Evaluated Configuration

The guidance documentation provides specific instructions for creating Configuration Profiles that configure the TOE to comply with the functions defined in the Security Target. The evaluated configuration included the devices listed below running Apple iOS 16 on iPhones:

- Apple device with CPU A11 Bionic: iPhone 8, iPhone 8 Plus, iPhone X
- Apple device with CPU A12 Bionic: iPhone XS, iPhone XS Max, iPhone XR
- Apple device with CPU A13 Bionic: iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone SE (2nd gen)
- Apple device with CPU A14 Bionic: iPhone 12 mini, iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max
- Apple device with CPU A15 Bionic: iPhone 13 mini, iPhone 13, iPhone 13 Pro, iPhone 13 Pro Max, iPhone SE (3rd gen), iPhone 14, iPhone 14 Plus
- Apple device with CPU A16 Bionic: iPhone 14 Pro, iPhone 14 Pro Max

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

All work units defined by CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the CFG_MDF-BIO-BT-MDMA-VPNC-WLANC_V1.0 (PP_MDF_V3.3, MOD_CPP_BIO_V1.1,

MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, and MOD_WLAN_CLI_V1.0) and PKG_TLS_V1.1 received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements as well as assurance activities. The evaluation was conducted based upon CEM Version 3.1 Revision 5. The evaluation determined the TOE to be CC Part 2 extended and Part 3 extended and to meet the assurance requirements defined by the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1.

Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1. The ST evaluation ensured that the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Apple iOS 16 iPhone products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and that the conclusion reached by the evaluation team was justified.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in

describing how to securely administer the TOE. Both the administrator and user guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activity specified in the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer can identify the evaluated TOE.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 and that the conclusion reached by the evaluation team was justified.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit and assurance activity specified in the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed/devised an independent set of tests as mandated by the protection profile.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 and that the conclusion reached by the evaluation team was justified.

Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1. The vendor provided security updates to the TOE during the evaluation; therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates, in line with the guidance provided in Scheme Policy Letter 15, fixed all known issues. The evaluation team ensured that the currently available version of the TOE does not contain known exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis and the evaluation team's performance of penetration tests.

The evaluators searched for publicly known vulnerabilities applicable to iOS using the following sources. The search was performed on multiple occasions on the following dates:

- 2023-06-02
- 2023-06-05
- 2023-07-17
- 2023-07-28
- 2023-08-04
- 2023-08-31
- 2023-09-17

Apple security content disclosure statements for releases of iOS 16 related to this evaluation are provided on the Apple support website.

In addition, the evaluation team used the following public sources:

- MITRE Common Vulnerabilities and Exposures (CVE) List
- NIST National Vulnerability Database (NVD)
- Cybersecurity and Infrastructure Security Agency (CISA)

using the following search terms:

- ios iphone
- ios apple
- ios 16.3
- ios core tls
- ios core crypto
- ios common crypto
- ios http
- ios https
- ios tcp
- ios ip

- ios bluetooth
- ios ipsec
- ios vpn
- ios mdm
- ios mobile
- ios touchid
- ios faceid
- broadcom wi-fi

The evaluator's CVE search found no vulnerabilities apart from the ones listed in the developer's security content disclosure statements, all of which have been fixed in subsequent releases of iOS.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 that the conclusion reached by the evaluation team was justified.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the testing defined by PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1 and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM and PP_MDF_V3.3, MOD_CPP_BIO_V1.1, MOD_BT_V1.0, MOD_MDM_AGENT_V1.0, MOD_VPN_CLI_V2.4, MOD_WLAN_CLI_V1.0 and PKG_TLS_V1.1and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documents listed in Section 6. No versions of the TOE and software, either earlier or later, were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11. Annexes

Not applicable.

12. Security Target

Apple iOS 16: iPhones Security Target (ST) Version 1.1, dated 2023-09-26.

13. Glossary

The following definitions are used throughout this document.

AA	Assurance Activity
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CDMA	Code Division Multiple Access
CCTL	Common Criteria Testing Laboratory—An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
CEM	Common Criteria Evaluation Methodology
CPU	Central Processing Unit
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EC	Elliptic Curve
EP	Extended Package (for a Protection Profile)
ETR	Evaluation Technical Report
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
GSM	Global System for Mobile Communication
HKDF	HMAC-based Extract-and-Expand Key Derivation Function

HMAC	Keyed-hash Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
LTE	Long-Term Evolution
MDM	Mobile Device Management
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PBKDF	Password Based Key Derivation Function
PP	Protection Profile
REK	Root Encryption Key
RFC	Request For Comments
SEP	Secure Enclave Processor
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation—A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
TLS	Transport Layer Security
TSF	TOE Security Functionality
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
VPN	Virtual Private Network
VR	Validation Report
WLAN	Wireless Local Area Network

14. Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- PP-Configuration for Mobile Device Fundamentals, Biometric enrollment and verification – for unlocking the device, Bluetooth, MDM Agents, Virtual Private Network (VPN) Clients, and WLAN Clients, Version 1.0, 2022-10-11
- Protection Profile for Mobile Device Fundamentals, Version 3.3, 2022-09-12
- collaborative PP-Module for Biometric enrolment and verification - for unlocking the device, Version 1.1, 2022-09-12
- PP-Module for Bluetooth, Version 1.0, 2021-04-15
- PP-Module for MDM Agents, Version 1.0, 2019-04-25
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 2022-03-31
- PP-Module for WLAN Clients, Version 1.0, 2022-03-31
- Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01
- Apple iOS 16: iPhones and Apple iPadOS 16: iPads Common Criteria Configuration Guide, Version 1.0, 2023-09-08
- Apple iOS 16: iPhones Security Target Version 1.1, 2023-09-26
- Apple iOS 16: iPhones Assurance Activity Report, Version 1.1, 2023-10-06