National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report for

Apple iPadOS 17: iPad

Report Number:	CCEVS-VR-VID11447-2025
Dated:	May 28, 2025
Version:	1.0

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

Department of Defense
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

Aerospace Corporation

Robert Wojcik, Ph.D.

Russ Fink

John Hopkins University Applied Physics lab

Common Criteria Testing Laboratory

Joachim Vandersmissen

Stephan Muller

Amr Said

Dick Sikkema

Hunter Barton

Walker Riley

atsec information security corporation

Austin, TX

Contents

1 EXECUTIVE SUMMARY 5

2 IDENTIFICATION 5

3 TOE ARCHITECTURE 7

4 ENVIRONMENTAL STRENGTHS 8

4.1 Security Audit 8
4.2 Cryptographic Support 8
4.3 User Data Protection 8
4.4 Identification and Authentication 8
4.5 Security Management 9
4.6 Protection of the TSF 9
4.7 TOE Access 9
4.8 Trusted Path/Channel 9

5 ASSUMPTIONS AND CLARIFICATION OF SCOPE 9

5.1 Assumptions 9
5.2 Clarification of Scope 10

6 DOCUMENTATION 10

7 IT PRODUCT TESTING 10

7.1 Test Configuration 11

8 TOE EVALUATED CONFIGURATION 11

8.1 Evaluated Configuration 11
8.2 Excluded Functionality 13

9 RESULTS OF THE EVALUATION 14

9.1 Evaluation of the Security Target (ST) (ASE) 14
9.2 Evaluation of the Development Activities (ADV) 14
9.3 Evaluation of the Guidance Activities (AGD) 14
9.4 Evaluation of the Life Cycle Support Activities (ALC) 15
9.5 Evaluation of the Test Documentation and the Test Activities (ATE) 15
9.6 Vulnerability Assessment Activity (AVA) 15
9.7 Summary of Evaluation Results 16

10 VALIDATOR COMMENTS/RECOMMENDATIONS 16

11 SECURITY TARGET 16

A ABBREVIATIONS AND ACRONYMS 17

B BIBLIOGRAPHY 18

List of Tables

TABLE 1: EVALUATION IDENTIFIERS 5
TABLE 2: TOE GUIDANCE 10
TABLE 3: DEVICES COVERED BY THE EVALUATION 11

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Apple iPadOS 17: iPad (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target ([ST]), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the Protection Profile, PP-Modules, and Functional Package identified in *Table 1*.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple iPadOS 17 executing on the following platforms: • iPad 9.7-inch (6th gen) (A10 Fusion processor)

	• iPad 10-2 inch (7th gen) (A10 Fusion processor) • iPad Pro 12.9-inch (2nd gen) (A10X Fusion processor) • iPad Pro 10.5-inch (A10X Fusion processor) • iPad mini (5th gen) (A12 Bionic processor) • iPad Air 10.5-inch (3rd gen) (A12 Bionic processor) • iPad (8th gen) (A12 Bionic processor) • iPad Pro 11-inch (A12X Bionic processor) • iPad Pro 12.9-inch (3rd gen) (A12X Bionic processor) • iPad Pro 11-inch (2nd gen) (A12Z Bionic processor) • iPad Pro 12.9-inch (4th gen) (A12Z Bionic processor) • iPad 10.2-inch (9th gen) (A13 Bionic processor) • iPad Air (4th gen) (A14 Bionic processor) • iPad 10.9-inch (10th gen) (A14 Bionic processor) • iPad mini (6th gen) (A15 Bionic processor) • iPad Pro 11-inch (3rd gen) (M1 processor) • iPad Pro 12.9-inch (5th gen) (M1 processor) • iPad Air (5th gen) (M1 processor) • iPad Pro 11-inch (4th gen) (M2 processor) • iPad Pro 12.9-inch (6th gen) (M2 processor)
Security Target	Apple iPadOS 17: iPad Security Target, Version 1.1, 2025-03-26
Sponsor & Developer	Apple Inc.
Completion Date	May 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
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, dated 2022-10-11, [CFG_MDF_BIO-BT-MDMA-VPNC-WLANC_V1.0] o [MDF]: Base-PP: Protection Profile for Mobile Device Fundamentals. Version 3.3 (PP_MDF_V3.3) as of 2022-09-12. o [BIO]: PP-Module: collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]. Version 1.1 (MOD_CPP_BIO_V1.1) as of 2022-09-12. o [BT]: PP-Module for Bluetooth. Version 1.0 (MOD_BT_V1.0) as of 2021-04-15.

	○ [Agent]: PP-Module for MDM Agents. Version 1.0 (MOD_MDM_AGENT_V1.0) as of 2019-04-25. ○ [VPNC]: PP-Module for Virtual Private Network (VPN) Clients. Version 2.4 (MOD_VPNC_V2.4) as of 2022-03-31. ○ [WLANC]: PP-Module for WLAN Clients. Version 1.0 (MOD_WLANC_V1.0) as of 2022-03-31. • [TLSPKG]: Functional Package for Transport Layer Security (TLS). Version 1.1 (PKG_TLS_V1.1) as of 2019-03-01.
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Evaluation Personnel	Joachim Vandersmissen, Stephan Mueller, Amr Said, Dick Sikkema, Hunter Barton, Walker Riley
Validation Personnel	Patrick W Mallet, Ph.D., Jerome F Myers, Ph.D., Seada Mohammed, Robert Wojcik, Ph.D., Russ Fink

3 TOE Architecture

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

The Target of Evaluation (TOE) is Apple iPadOS 17: iPad, which is a series of Apple iPad mobile devices running the iPadOS 17 operating system, a Mobile Device Management (MDM) Agent, VPN client, and WLAN client components, which are included on the mobile devices.

The TOE operating system manages the device hardware, provides MDM Agent functionality, and provides the technologies required to implement native applications. It provides a built-in MDM framework application programmer interface (API), giving management features that may be utilized by external MDM solutions, allowing enterprises to use profiles to control some of the device settings.

The TOE operating system provides a consistent set of capabilities allowing the supervision of enrolled devices. This includes the preparation of devices for deployment, the subsequent management of the devices, and the termination of management.

The operating system part of the TOE acts as an intermediary between the underlying hardware and the apps running on the TOE. Apps do not talk to the underlying hardware directly. Instead, they communicate with the hardware through a set of well-defined system interfaces. These interfaces make it easy to write apps that work consistently on devices having different hardware capabilities.

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

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. When designing apps, one should investigate the technologies in this layer first to see if they meet the needs of the developer.

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 is 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. Moreover, this layer 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.

The **Core OS layer** contains the low-level features that most other technologies are built upon. This layer provides the security-related frameworks: Generic Security Services Framework for services specified in RFC 2743 and RFC 4401; Local Authentication Framework, Network Extension Framework for support of VPN tunnels, Security Framework for providing the Common Crypto library and managing certificates, cryptographic keys and trust policies and System Framework for providing the kernel environment and low-level UNIX interfaces.

4 Environmental Strengths

The TOE provides the following security functions as described in the Security Target ([ST]).

4.1 Security Audit

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.

4.2 Cryptographic Support

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

- Apple corecrypto Module v14.0 [Apple silicon, User, Software, SL1]
- Apple corecrypto Module v14.0 [Apple silicon, Kernel, Software, SL1]
- Apple corecrypto Module v14.0 [Apple silicon, Secure Key Store, Hardware, SL2]

4.3 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 keychain, 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

4.4 Identification and Authentication

The TOE provides user authentication using a passcode or biometric (fingerprint or face) except for Medical ID information, answering calls, making emergency calls, using the cameras, control center, flashlight or notification center.

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.

4.5 Security Management

The security functions listed in the Security Target can be managed either by the user or by an authorized administrator through a Mobile Device Management (MDM) system. The Security Target identifies the functions that can be managed and indicates if the management can be performed by the user, by the authorized administrator, or both.

4.6 Protection of the TSF

The TOE implements the following protection of TSF data functions:

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

4.7 TOE Access

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

4.8 Trusted Path/Channel

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, TLS (v1.1, v1.2), IPsec, Bluetooth (v5.0, v5.3).

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, as listed in *Table 1.*

The TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

- Mobile device users are not willfully negligent or hostile and use the device within compliance of a reasonable Enterprise security policy.
- The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
- TOE administrators are competent, trusted personnel who are not careless, willfully negligent, or hostile and abide by guidance documentation.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

5.2 Clarification of Scope

As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the *PP, PP-Modules*, and Functional Package specified in *Table 1.*

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Apple iPadOS 17: iPad Security Target, March 20, 2025 (ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

Table 2: TOE Guidance

Reference	Document	Location
[CCGUIDE]	Apple iOS 17: iPhone and Apple iPadOS 17: iPad Common Criteria Configuration Guide	https://www.niap-ccevs.org/product/11446 https://www.niap-ccevs.org/products/11447

7 IT Product Testing

This section describes the testing efforts of the evaluation team.

A non-proprietary description of the tests performed, and their results is provided in the following document:

- *Assurance Activity Report Apple iPadOS 17: iPad*, Version 1.1, 2025-05-16 ([AAR]).

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the PPs, PP-Modules, and functional packages listed in *Table 1.*

The evaluation team devised a Test Plan based on the Test Activities specified in the above *PP* and Functional Package. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX, Germany CCTL in Munich, Germany and at Apple facility in Cupertino, CA, from January 2024 to March 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising Apple iPadOS 17 running on platforms listed in *Table 3*. The Assurance Activities Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE.

8 TOE Evaluated Configuration

8.1 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 devices running iPadOS 17 operating system as detailed in *Table 1.*

Table 3: Devices Covered by the Evaluation

Processor	Device Name	Model Number
A10 Fusion	iPad 9.7-inch (6th gen)	A1893
		A1954
	iPad 10.2-inch (7th gen)	A2197
		A2198 (Hong Kong)
		A2199
		A2200
A10X Fusion	iPad Pro 12.9-inch (2nd gen)	A1670
		A1671
		A1821 (China)
	iPad Pro 10.5-inch	A1701
		A1709
		A1852 (China)
A12 Bionic	iPad mini (5th gen)	A2124
		A2125 (China)
		A2126
		A2133
	iPad Air 10.5-inch (3rd gen)	A2123
		A2152
		A2153
		A2154 (China)
	iPad 10.2-inch (8th gen)	A2270
		A2428

		A2429
		A2430 (China)
A12X Bionic	iPad Pro 11-inch	A1934 (US/CA)
		A1979 (China)
		A1980
		A2013 (US/CA)
	iPad Pro 12.9-inch (3rd gen)	A1876
		A1895
		A1983 (China)
		A2014 (US/CA)
A12Z Bionic	iPad Pro 11-inch (2nd gen)	A2068
		A2228
		A2230
		A2231 (China)
	iPad Pro 12.9-inch (4th gen)	A2069
		A2229
		A2232
		A2233 (China)
A13 Bionic	iPad 10.2-inch (9th gen)	A2602
		A2603
		A2604
		A2605
A14 Bionic	iPad Air (4th gen)	A2072 (Global)
		A2316
		A2324 (US/CA)
		A2325 (China)
	iPad 10.9 inch (10th gen)	A2696
		A2757
		A2777 (China)
A15 Bionic	iPad mini (6th gen)	A2567
		A2568
		A2569
M1	iPad Pro 11-inch (3rd gen)	A2301
		A2377
		A2459
		A2460

	iPad Pro 12.9-inch (5th gen)	A2378
		A2379
		A2461
		A2462
	iPad Air (5th gen)	A2588
		A2589
		A2591
M2	iPad Pro 11-inch (4th gen)	A2435
		A2759
		A2761
		A2762
	iPad Pro 12.9-inch (6th gen)	A2436
		A2437
		A2764
		A2766

8.2 Excluded Functionality

Apple iPadOS 17: iPad additionally includes the following features that are not part of the evaluated TOE because they are outside the scope of the functionality described by the TOE's conformance claims:

- **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.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Apple iPadOS 17: iPad ([ETR]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the PPs, PP-Modules, and functional packages listed in *Table 1.*

The evaluation determined the TOE satisfies the conformance claims made in the Apple iPadOS 17: iPad Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the *PP, PP-Modules*, and *Functional Package* identified in *Table 1.*

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and each work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, and ASE_TSS.1 CEM. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed *PP, PP-Modules*, and *Functional Package* identified in, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development Activities (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed *PPs, PP-Modules*, and *Functional Packages* for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each AGD_OPE.1 and AGE_PRE.1 work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit to the extent possible given the evaluation evidence required by the claimed *PPs, PP-Modules*, and *Functional Packages*. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team performed each ATE assurance activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed *PPs, PP-Modules*, and *Functional Packages* and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed *PPs, PP-Modules*, and *Functional Packages*. This comprised a search of public vulnerability databases.

The evaluator searched for publicly known vulnerabilities applicable to the TOE release and its subsequent releases using the following sources:

- MITRE Common Vulnerabilities and Exposures (CVE) List:
  - https://cve.mitre.org/cve/search_cve_list.html
- National Vulnerability Database:
  - https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities Catalog:
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Keywords used in CVE search:

- ipados ipad
- ipados apple
- ipados 17.2
- ipados core tls
- ipados core crypto
- ipados common crypto
- ipados http
- ipados https
- ipados tcp
- ipados ip
- ipados bluetooth
- ipados ipsec
- ipados vpn
- ipados mdm
- ipados mobile
- ipados touchid
- ipados faceid
- broadcom wi-fi

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches on the dates 03/03/2025 and 05/12/2025. The results of these searches did not identify any vulnerabilities.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed *PPs, PP-Modules*, and *Functional Packages*. Furthermore, the evaluation team's testing demonstrates the accuracy of the claims in the ST.

The validation team'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 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 Apple iOS 17: iPhone and Apple iPadOS 17: iPad Common Criteria Configuration Guide, Version 1.0, 2025-03-26.

No versions of the TOE and software, either earlier or later are covered by the scope of this evaluation. 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. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 8.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The ST for this product's evaluation is Apple iPadOS 17: iPad Security Target, Version 1.1, 2025-03-26 ([ST]).

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

B Bibliography

The validation team used the following documents to produce this VR:

[CCPART1]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
[CCPART2]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
[CCPART3]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
[AAR]	Assurance Activities Report Apple iPadOS17: iPad, Version 1.1, 2025-05-16
[CEM]	Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
[CCGUIDE]	Apple iOS 17: iPhone and Apple iPadOS 17: iPad Common Criteria Configuration Guide, Version 1.0, 2025-03-26
[CFG_MDF_BIO-BT-MDMA-VPNC-WLAN_V1.0]	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, dated 2022-10-11
[BIO]	PP-Module for collaborative PP-Module for Biometric enrolment and verification - for unlocking the device, Version 1.1, 2022-09-12.
[BT]	PP-Module Bluetooth, Version 1.0, 2021-04-15.
[ETR]	Evaluation Technical Report Apple iPadOS17: iPad, Version 1.1, 2025-05-16
[MDF]	Protection Profile for Mobile Device Fundamentals. Version 3.3, 2022-09-12.
[TLSPKG]	Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01.
[ST]	Apple iPadOS 17: iPad Security Target, Version 1.1, 2025-03-26
[VPNC]	PP-Module for Virtual Private Network (VPN) Clients. Version 2.4, 2022-03-31
[WLANC]	PP-Module for WLAN Clients. Version 1.0, 2022-03-31.