National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
Apple macOS 14 Sonoma

Report Number: CCEVS-VR-VID11584-2025
Dated: 12/23/2025
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

Jerome Myers, Ph.D.

Patrick Mallett, Ph.D.

Seada Mohammed

Aerospace Corporation

Sheldon Durrant

Randy Heimann

The MITRE Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Nil Folquer

Lightship Security USA, Inc.

Table of Contents

1. Executive Summary 1
2. Identification 2
3. Architectural Information 4
   3.1. TOE Evaluated Configuration 4
   3.2. Physical Boundary 6
   3.3. Required Non-TOE Hardware, Software, and Firmware 6
4. Security Policy 7
   4.1. Security Audit 7
   4.2. User Data Protection 7
   4.3. Identification and Authentication 7
   4.4. Security Management 8
   4.5. Protection of the TSF 8
   4.6. Trusted Path/Channels 8
   4.7. TOE Access 8
   4.8. Cryptographic Support 8
5. Assumptions 9
6. Clarification of Scope 10
7. Documentation 11
8. IT Product Testing 12
   8.1. Developer Testing 12
   8.2. Evaluation Team Independent Testing 12
   8.3. Evaluated Configuration 12
9. Results of the Evaluation 14
   9.1. Evaluation of Security Target (ASE) 14
   9.2. Evaluation of Development Documentation (ADV) 14
   9.3. Evaluation of Guidance Documents (AGD) 14
   9.4. Evaluation of Life Cycle Support Activities (ALC) 15
   9.5. Evaluation of Test Documentation and the Test Activity (ATE) 15
   9.6. Vulnerability Assessment Activity (VAN) 15
   9.7. Summary of Evaluation Results 16
10. Validator Comments 17

11. Annexes 18
12. Security Target 19
13. Glossary 20
14. Acronym List 21
15. Bibliography 22

List of Tables

Table 1: Evaluation Identifiers 2
Table 2: Hardware Platforms – Apple Silicon 4
Table 3: TOE Operational Environment 6
Table 4: Assumptions 9

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Apple macOS 14 Sonoma provided by Apple Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) 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 Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in December 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements of the PP-Configuration for PP-Configuration for General Purpose Operating System, Bluetooth, and Wireless Local Area Network Clients; Protection Profile for General Purpose Operating Systems, Version 4.3; PP-Module: PP-Module for Bluetooth, Version 1.0; PP-Module: PP-Module for WLAN Clients, Version 1.0; and Functional Package for Transport Layer Security (TLS), Version 1.1.

The TOE is Apple macOS 14 Sonoma. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR 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 ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, 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 of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Security Target and analysis performed by the Validation Team.

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) 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 Validated Products List.

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

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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
Evaluated Product	Apple macOS 14 Sonoma
Sponsor and Developer	Apple Inc. One Apple Park Way Cupertino, CA 95014
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	PP-Configuration for PP-Configuration for General Purpose Operating System, Bluetooth, and Wireless Local Area Network Clients This PP-Configuration includes the following components: Base-PP: Protection Profile for General Purpose Operating Systems, Version 4.3 PP-Module: PP-Module for Bluetooth, Version 1.0 PP-Module: PP-Module for WLAN Clients, Version 1.0 Functional Package for Transport Layer Security (TLS), Version 1.1
ST	Apple macOS 14 Sonoma Security Target, v1.7, December 19, 2025.
Evaluation Technical Report	Apple macOS 14 Sonoma Evaluation Technical Report, v1.1, December 19, 2025
Conformance Result	CC Part 2 extended, CC Part 3 extended
Evaluation Personnel	Kenji Yoshino Nil Folquer
CCEVS Validators	Jerome Myers, Ph.D. Patrick Mallett, Ph.D. Seada Mohammed Sheldon Durrant Randy Heimann

3. Architectural Information

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

The TOE is a general-purpose operating system (GPOS) for Apple Mac computers containing Apple Silicon series processors and provides wireless LAN and Bluetooth functionality.

3.1. TOE Evaluated Configuration

The TOE is in the evaluated configuration when it is configured according to *Apple macOS 14 Sonoma Common Criteria Guide* and running on a hardware platform listed in Table 2.

Table 2: Hardware Platforms – Apple Silicon

Marketing Name	Model	Model Identifier	Processor (Micro Architecture)	Security Chip	BT Version (BT/WiFi Chip)
2023					
MacBook Pro (16-inch, 2023)	A2780	Mac14,6	M2 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac14,10	M2 Pro (ARMv8.6-A)		
MacBook Pro (14-inch, 2023)	A2779	Mac14,5	M2 Max (ARMv8.6-A)	SEP v2.0	5.3 (4388)
		Mac14,9	M2 Pro (ARMv8.6-A)		
Mac mini (M2 Pro, 2023)	A2816	Mac14,12	M2 Pro (ARMv8.6-A)	SEP v2.0	5.3 (4388)
Mac mini (M2, 2023)	A2686	Mac14,3	M2 (ARMv8.6-A)	SEP v2.0	5.3 (4388)
2022					
MacBook Pro (13-inch, M2, 2022)	A2338	Mac14,7	M2 (ARMv8.6-A)	SEP v2.0	5.0 (4378)

Marketing Name	Model	Model Identifier	Processor (Micro Architecture)	Security Chip	BT Version (BT/WiFi Chip)
MacBook Air (M2, 2022)	A2861	Mac14,2	M2 (ARMv8.6-A)	SEP v2.0	5.0 (4387)
Mac Studio (2022)	A2615	Mac13,2	M1 Ultra (ARMv8.5-A)	SEP v2.0	5.0 (4387)
		Mac13,1	M1 Max (ARMv8.5-A)		
2021					
MacBook Pro (16-inch, 2021)	A2485	MacBookPro18,2	M1 Max (ARMv8.5-A)	SEP v2.0	5.0 (4387)
		MacBookPro18,1	M1 Pro (ARMv8.5-A)		
MacBook Pro (14-inch, 2021)	A2442	MacBookPro18,4	M1 Max (ARMv8.5-A)	SEP v2.0	5.0 (4387)
		MacBookPro18,3	M1 Pro (ARMv8.5-A)		
iMac (24-inch, M1, 2021)	A2438	iMac21,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
	A2439	iMac21,2			
2020					
Mac mini (M1, 2020)	A2348	Macmini9,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
MacBook Air (M1, 2020)	A2337	MacBookAir10,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)
MacBook Pro (13-inch, M1, 2020)	A2338	MacBookPro17,1	M1 (ARMv8.5-A)	SEP v2.0	5.0 (4378)

3.2. Physical Boundary

The physical boundary of the TOE is the installation image which includes both macOS and sepOS installed on Apple devices. If required, the Administrator can leverage the built-in update feature to check for and install the same version of the TOE or newer version. Additionally, the TOE can be manually installed using the built-in "App Store".

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the components listed in Table 3 in the operational environment:

Table 3: TOE Operational Environment

Component	Description
Hardware platform	See section 3.1
Apple Update Server	Server that allows the TOE to download updates
Smart Card, Smart Card Reader	An encrypted card that allows the TOE to authenticate a user when used with smart card reader devices.
NTP Server	Server that allows the TOE to synchronise its time
Wireless Access Point	Access point for the TOE to connect to for WLAN connectivity capable of mediating 802.1X authentication.
RADIUS server	A RADIUS server capable of providing 802.1X services.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified by the conformance claims defined in 1.3. Audit events are generated for the following audit functions:

1. Start-up and shut-down of the audit functions,
2. Authentication events (Success/Failure),
3. Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes),
4. Privilege or role escalation events (Success/Failure),
5. Administrator or root-level access events (Success/Failure),
6. Events related to Bluetooth connections and user authorizations,
7. Events related to connections to Wi-Fi networks and associated user authentications,
8. Attempts to load and revoke X.509 certificates; and,
9. Execution of TSF-self tests.

Each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event.

4.2. User Data Protection

The TOE implements access controls that prevent unprivileged users from accessing files and directories owned by other users.

4.3. Identification and Authentication

All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports:

1. password-based authentication,
2. authentication based on username and a PIN that releases asymmetric key stored in OE-protected storage.

The TOE will lock out user accounts after a defined number of unsuccessful authentication attempts have been met. The TOE supports Bluetooth Secure Simple Pairing (SSP). It requires user authorization and mutual authentication during pairing. It also discards pairing attempts and session initialization from Bluetooth devices to which an active session pre-exists. The TOE requires explicit user authorization when pairing with an untrusted device.

The TOE also supports the use of X.509 certificates for the purpose of identifying itself and/or its users for TLS connections as well as for connecting to Wi-Fi networks using EAP-TLS.

4.4. Security Management

The TOE can perform management functions. The administrator has full access to carry out all management functions; whereas the user will have limited privileges.

4.5. Protection of the TSF

The TOE implements the following protection of TSF data functions:

1. Access Controls.
2. Address space layout randomization (ASLR) with 16 bits of entropy.
3. Stack buffer overflow protection.
4. Verification of integrity of the boot-chain and operating system executable code.
5. Trusted software updates using digital signatures.

4.6. Trusted Path/Channels

The TOE supports TLS v1.2 for trusted channel communications. The TOE uses TLS to securely communicate with the Apple Update Server. The TOE enforces encryption when transmitting data over Bluetooth for both BR/EDR and LE and terminates the connection if the connected device stops encrypting. The TOE enforces 802.1X EAP-TLS authentication to wireless access points and protects wireless traffic using encryption when connecting via the wireless LAN client.

4.7. TOE Access

Before establishing a user session, the TOE will display an advisory warning message regarding unauthorized use of the OS.

4.8. Cryptographic Support

The TOE includes the Apple corecrypto v14.0 cryptographic libraries and is supported by the onboard Apple SEP Hardware for performing user space, kernel space, and SEP cryptographic operations. In addition, it uses a software and hardware noise source for entropy generation. The TOE implements TLS 1.2 for secure communications with remote servers. The Bluetooth hardware implements the AES-CCM-128 cryptographic functionality used when connecting to Bluetooth devices. The TOE implements WPA3 to secure 802.11 wireless traffic protected using AES-GCMP-256 cryptographic algorithms.

5. Assumptions

Table 4: Assumptions

Identifier	Description	PP Origin
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.	PP_OS_V4.3
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.	PP_OS_V4.3
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.	PP_OS_V4.3
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.	MOD_WLANC_V1.0
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	MOD_WLANC_V1.0

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP, Modules, Functional Package, and Supporting Documents as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices 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 clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in the PP, Modules, Functional Package, and Supporting Documents and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the PP, Modules, Functional Package, and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Apple macOS 14 Sonoma Common Criteria Guide*, v1.2, *December 19, 2025*

Any additional customer documentation provided with the product or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Apple macOS 14 Sonoma Assurance Activity Report* provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from April 2025 until October 2025. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The TOE was configured according to *Apple macOS 14 Sonoma Common Criteria Guide.* The test environment was limited to the system(s) necessary to test the specific TOE functionality. For example, when Bluetooth was being tested, the Bluetooth peer was the only test system in use. Specific details are contained in the proprietary Detailed Test Report.

The following tools were used for testing:

- bm-search
- lldb
- FreeRADIUS
- Dnsmasq
- gl-tools
- OpenSSL
- Wireshark
- tcpdump
- ntpd
- Profile Tuning Suite
- Sweyntooth

- ESP-WROOM-32
- Nordic nRF52840
- Hostapd
- PacketLogger

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

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 and CEM Version 3.1 Revision 5. The evaluation determined Apple macOS 14 Sonoma to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in the PP, Modules, Functional Package, and Supporting Documents.

9.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured 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 macOS 14 Sonoma that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was 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.

9.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was 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.

9.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. 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. All of the 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 was 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.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was 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.

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

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was 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.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Apple macOS 14 Sonoma Vulnerability Assessment*, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on December 8, 2025, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- MITRE CVE database: https://cve.mitre.org/cve/search_cve_list.html
- CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Vendor Security Advisories

The Evaluation team performed a search using the following CPE[1]:

[1] Apple includes libraries, components, and applications under the macOS CPE, so the above search encompasses all components of the TOE. To address vulnerabilities discovered as part of the initial public vulnerability search, the TOE was updated from version 14.7.4 to 14.8.2; however, the original CPE was retained for tracking and rationale purposes (i.e., CVE rationale and regression testing).

- cpe:2.3:o:apple:macos:14.7.4:*:*:*:*:*:*:*

The Evaluation team also performed a search using the following keywords:

- macOS Sonoma
- macOS 14

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was 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.

9.7. 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 test activities also demonstrated 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 performed the Evaluation Activities in the PP, Modules, Functional Package, and Supporting Documents; and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Apple macOS 14 Sonoma Security Target, v1.7, December 19, 2025.

13. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** 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.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **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.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** 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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *PP-Configuration for General Purpose Operating System, Bluetooth, and Wireless Local Area Network Clients, Version 1.0 2025-05-12*
6. *Protection Profile for General Purpose Operating Systems*, Version 4.3, 2022-09-27
7. *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 2019-03-01
8. *PP-Module for Bluetooth*, Version 1.0, 2021-04-15
9. *Supporting Document Mandatory Technical Document PP-Module for Bluetooth, Version 1.0*, 2021-04-15
10. *PP-Module for WLAN Clients*, Version 1.0
11. *Supporting Document Mandatory Technical Document PP-Module for WLAN Clients*, Version 1.0
12. *Apple macOS 14 Sonoma Security Target*, v1.7
13. *Apple macOS 14 Sonoma Common Criteria Guide*, v1.2
14. *Apple macOS 14 Sonoma Assurance Activity Report*, v1.1
15. *Apple macOS 14 Sonoma Vulnerability Assessment*, v1.1
16. *Apple macOS 14 Sonoma Evaluation Technical Report*, v1.1
17. *Apple macOS 14 Sonoma Detailed Test Report*, v1.1
18. *Apple macOS 14 Sonoma Test Evidence*, v1.0