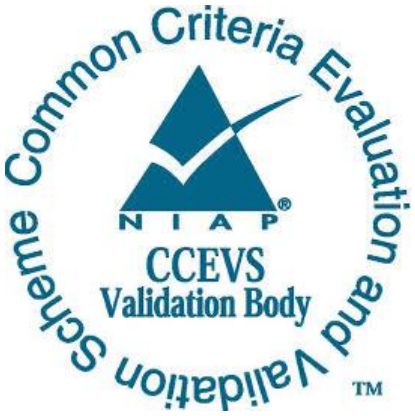
# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme




# Validation Report

# Apple macOS 13 Ventura

**Report Number:** **CCEVS-VR-VID11347-2024**
**Dated:** **February 6, 2024**
**Version:** **1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 2089**

**Department of Defense**
**ATTN: NIAP, SUITE: 6982**
**9800 Savage Road**
**Fort Meade, MD 20755-6982**

# ACKNOWLEDGEMENTS

**Validation Team**

Jim Donndelinger
Patrick Mallett, Ph.D.
Mike Quintos
Fernando Guzman
*The Aerospace Corporation*

**Common Criteria Testing Laboratory**
King Ables
Stephan Mueller
Joachim Vandersmissen
Walker Riley
Markus Engqvist
Alex Gong
*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 the Apple macOS 13 Ventura general purpose operating system (GPOS). 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. This VR applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

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 February 2024. 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 General Purpose Operating Systems and Bluetooth, Version 1.0, 2021-04-15; (CFG_GPOS-BT_V1.0)
    - Base PP: Protection Profile for General Purpose Operating Systems. Version 4.2.1, 2019-04-22, (PP_GPOS_V4.2.1)
    - PP Module: PP-Module for Bluetooth, Version 1.0, 2021-04-15, (MOD_BT_V1.0)

The TOE is Apple macOS 13 Ventura.

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 Evaluation Activities (EA) of the aforementioned Protection Profiles. 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 General Purpose Operating Systems and Bluetooth, Version 1.0, 2021-04-15; (CFG_GPOS-BT_V1.0)

- Base PP: Protection Profile for General Purpose Operating Systems. Version 4.2.1, 2019-04-22, (PP_GPOS_V4.2.1)
- PP Module: PP-Module for Bluetooth, Version 1.0, 2021-04-15, (MOD_BT_V1.0)

have been met.

The technical information included in this report was obtained from the Apple macOS 13 Ventura Security Target, Version 1.1, 1/12/2024

# 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 macOS 13 Ventura |
| **PP** | • PP-Configuration for General Purpose Operating Systems and Bluetooth, Version 1.0, 2021-04-15; (CFG_GPOS-BT_V1.0)<br>o Base PP: Protection Profile for General Purpose Operating Systems. Version 4.2.1, 2019-04-22, (PP_GPOS_V4.2.1) |

| Item | Identifier |
|---|---|
| | ○ PP Module: PP-Module for Bluetooth, Version 1.0, 2021-04-15, (MOD_BT_V1.0) |
| **ST** | Apple macOS 13 Ventura Security Target [ST], Version 1.1, dated 2024-01-12 |
| **ETR** | Evaluation Technical Report for a Target of Evaluation Apple macOS 13 Ventura, Version 1.1, dated 2024-01-12 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 extended |
| **Sponsor** | Apple Inc. |
| **Developer** | Apple Inc. |
| **CCTL** | atsec information security corporation, Austin, TX |
| **CCEVS Validators** | Jim Donndelinger<br>Patrick Mallett, Ph.D.<br>Mike Quintos<br>Fernando Guzman |

# 3 Architectural Information

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

The TOE is the Apple macOS 13 Ventura general purpose operating system which is tightly integrated with hardware and runs on Apple iMac, MacBook Air, MacBook Pro, Mac mini, Mac Pro, and Mac Studio computers. The macOS Ventura operating system is a Unix-based graphical operating system. The macOS core is a POSIX compliant operating system built on top of the XNU kernel with standard Unix facilities available from the command line interface. The TOE includes Bluetooth communication—both Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) and Low Energy (LE). A portion of the TOE's Bluetooth functionality is implemented in hardware.

The tested version of the TOE is Apple macOS 13.2.1.

## 3.1 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 TOE hardware consists of two groups: Apple silicon Macs and “Intel with T2” Macs. The Apple silicon Macs use an Apple silicon System on a Chip (SoC) and the “Intel with T2” Macs use an Intel processor with Apple

T2 Security Chip. The evaluation covers the following Apple silicon and T2 systems running macOS 13.2.1 operating system as detailed in Table 1. Apple silicon processors start with the letter M and the Intel processors start with either Core or Xeon. Bluetooth is abbreviated as BT.

**Table 1: Devices Covered by the Evaluation**

| Marketing Name | Model # | Model Identifier | Processor | microArch | Security Chip | BT | BT 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 | SEP v2.0 | 5.3 | 4388 |
| 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 | SEP v2.0 | 5.3 | 4388 |
| 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 |
| MacBook Air (M2, 2022) | A2861 | Mac14,2 | M2 | ARMv8.6-A | SEP v2.0 | 5.0 | 4387 |
| Mac Studio | A2615 | Mac13,2 | M1 Ultra | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| | A2615 | Mac13,1 | M1 Max | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| **2021** | | | | | | | |
| MacBook Pro (16-inch, 2021) | A2485 | MacBookPro 18,2 | M1 Max | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| | | MacBookPro 18,1 | M1 Pro | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| MacBook Pro (14-inch, 2021) | A2442 | MacBookPro 18,4 | M1 Max | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| | | MacBookPro 18,3 | M1 Pro | ARMv8.5-A | SEP v2.0 | 5.0 | 4387 |
| iMac (24-inch, M1, 2021) | A2438 | iMac21,1 | M1 | ARMv8.5-A | SEP v2.0 | 5.0 | 4378 |
| | A2439 | iMac21,2 | M1 | ARMv8.5-A | SEP v2.0 | 5.0 | 4378 |

| Marketing Name | Model # | Model Identifier | Processor | microArch | Security Chip | BT | BT Chip |
|---|---|---|---|---|---|---|---|
| **2020** | | | | | | | |
| Mac mini (M1, 2020) | A2348 | Macmini9,1 | M1 | ARMv8.5-A | SEP v2.0 | 5.0 | 4378 |
| MacBook Air (M1, 2020) | A2337 | MacBookAir 10,1 | M1 | ARMv8.5-A | SEP v2.0 | 5.0 | 4378 |
| MacBook Pro (13-inch, M1, 2020) | A2338 | MacBookPro 17,1 | M1 | ARMv8.5-A | SEP v2.0 | 5.0 | 4364 |
| MacBook Air (Retina, 13-inch, 2020) | A2179 | MacBookAir 9,1 | Core i5-1030NG7<br>Core i7-1060NG7 | Ice Lake | T2 | 5.0 | 4377 |
| MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports) | A2251 | MacBookPro 16,2 | Core i5-1038NG7<br>Core i7-1068NG7 | Ice Lake | T2 | 5.0 | 4377 |
| MacBook Pro (13-inch, 2020, Two Thunderbolt 3 ports) | A2289 | MacBookPro 16,3 | Core i5-8257U<br>Core i7-8557U | Coffee Lake | T2 | 5.0 | 4377 |
| iMac (Retina 5K, 27-inch, 2020) | A2115 | iMac20,1<br>iMac20,2 | Core i5-10500<br>Core i5-10600<br>Core i7-10700K<br>Core i9-10910 | Comet Lake | T2 | 5.0 | 4364 |
| **2019** | | | | | | | |
| MacBook Air (Retina, 13-inch, 2019) | A1932 | MacBookAir 8,2 | Core i5-8210Y | Amber Lake | T2 | 4.2 | 4355 |
| MacBook Pro (13-inch, 2019, Four Thunderbolt 3 ports) | A1989 | MacBookPro 15,2 | Core i5-8279U<br>Core i7-8569U | Coffee Lake | T2 | 5.0 | 4364 |
| MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports) | A2159 | MacBookPro 15,4 | Core i5-8257U<br>Core i7-8557U | Coffee Lake | T2 | 5.0 | 4377 |
| MacBook Pro (15-inch, 2019) | A1990 | MacBookPro 15,1<br>MacBookPro 15,3 | Core i7-9750H<br>Core i9-9880H<br>Core i9-9980HK | Coffee Lake | T2 | 5.0 | 4364 |
| MacBook Pro (16-inch, 2019) | A2141 | MacBookPro 16,1<br>MacBookPro 16,4 | Core i7-9750H<br>Core i9-9880H<br>Core i9-9980HK | Coffee Lake | T2 | 5.0 | 4377 |
| Mac Pro (2019) | A1991 | MacPro7,1 | Xeon W-3223<br>Xeon W-3235<br>Xeon W-3245<br>Xeon W-3265M<br>Xeon W-3275M | Cascade Lake | T2 | 5.0 | 4364 |

| Marketing Name | Model # | Model Identifier | Processor | microArch | Security Chip | BT | BT Chip |
|---|---|---|---|---|---|---|---|
| Mac Pro (2019 Rack) | A2304 | MacPro7,1 | Xeon W-3223<br>Xeon W-3235<br>Xeon W-3245<br>Xeon W-3265M<br>Xeon W-3275M | Cascade Lake | T2 | 5.0 | 4364 |
| **2018** | | | | | | | |
| MacBook Air (Retina, 13-inch, 2018) | A1932 | MacBookAir 8,1 | Core i5-8210Y | Amber Lake | T2 | 4.2 | 4355 |
| Mac mini (2018) | A1993 | Macmini8,1 | Core i5-8500B<br>Core i7-8700B | Coffee Lake | T2 | 5.0 | 4364 |
| MacBook Pro (15-inch, 2018) | A1990 | MacBookPro 15,1<br>MacBookPro 15,3 | Core i7-8750H<br>Core i7-8850H<br>Core i9-8950HK | Coffee Lake | T2 | 5.0 | 4364 |
| MacBook Pro (13-inch, 2018, Four Thunderbolt 3 ports) | A1989 | MacBookPro 15,2 | Core i5-8259U<br>Core i7-8559U | Coffee Lake | T2 | 5.0 | 4364 |
| **2017** | | | | | | | |
| iMac Pro (2017) | A1862 | iMacPro1,1 | Xeon W-2140B<br>Xeon W-2150B<br>Xeon W-2170B<br>Xeon W-2190B | Skylake | T2 | 5.0 | 4364 |

## 3.2 Physical Scope of the TOE

The TOE includes both hardware and software running on the Macs listed in Appendix A.1 “Hardware Platforms Covered by this Evaluation” of the ST. These Macs are organized into the following two groups:

- Apple silicon Macs
- “Intel with T2” Macs

The Apple silicon Macs group represents all systems listed in Appendix A.1 of the Security Target as well as the table above that use an Apple silicon System on a Chip (Soc). The “Intel with T2” Macs group represents all systems listed in Appendix A.1 that use an Intel processor with the Apple T2 Security Chip. These groups have implementation differences as indicated in the ST.

The TOE also includes the TOE documentation providing information for installing, configuring, and maintaining the evaluated configuration titled:

- Apple macOS 13 Ventura Common Criteria Configuration Guide, Version 1.1

The Macs in this evaluation contain the Apple Secure Enclave. The Secure Enclave contains the Secure Enclave Processor (SEP) and a true random number generator (TRNG). The SEP runs sepOS. sepOS is included with macOS and is in the TOE boundary.

On Apple silicon Macs, the Secure Enclave is located on the SoC along with the application processor. On "Intel with T2" Macs, the Secure Enclave is located on the T2 chip.

Both the Apple silicon and "Intel with T2" Macs include a Broadcom chip that implements part of the Bluetooth functionality; the chip model depends on the hardware platform and are also listed in Appendix A.1 of the ST.

## 3.3 Un-evaluated Functionality

The following product functionality is not included in the CC evaluation.

- 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. It is designed to enhance the security on these on-line Apple accounts. This feature is outside the scope of the evaluation.
- Bonjour – Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network. This feature is outside the scope of the evaluation.
- VPN Split Tunnel – VPN split tunnel is not included in the evaluation and must be disabled.
- Siri – Siri supports some commands related to configuration settings. This feature is not included in the evaluation and must be disabled.

# 4 Security Policy

The TOE implements the security functions required by Protection Profile for General Purpose Operating Systems. Version 4.2.1 and PP-Module for Bluetooth, Version 1.0. The security functions the TOE implements are summarized as follows.

## 4.1 Security Audit

The TOE generates audit records for the following auditable events:

- Start-up and shutdown of the audit functions
- Authentication events (success/failure)
- Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)
- Privilege or role escalation events (success/failure)

The TOE also generates audit records for the following Bluetooth auditable events:

- Failed user authorization of Bluetooth device and for local Bluetooth service

- Initiation and failure of Bluetooth connection

## 4.2 Cryptographic Support

The TOE includes the Apple corecrypto v13.0 cryptographic libraries listed below for performing user space, kernel space, and Secure Enclave Processor (SEP) cryptographic operations. The TOE implements TLS 1.2 for secure communications with remote servers.

The Bluetooth hardware implements the bulk AES-CCM-128 cryptographic functionality used when connecting to Bluetooth devices.

Apple silicon

- 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 silicon, Secure Key Store, Hardware, SL2]

Intel with T2

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

## 4.3 User Data Protection

The TOE implements access controls that prevent unprivileged users from accessing files and directories owned by other users. The TOE uses the Apple File System (APFS), which provides access control to data. The TOE provides the following file system security schemes: sandbox entitlements, POSIX access control lists (ACLs), Unix (BSD) permissions, and per-file BSD flags that override Unix permissions.

## 4.4 Identification and Authentication

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

- Password-based authentication
- Authentication based on username and a PIN that releases an asymmetric key stored in Operational Environment (OE) protected storage

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.

## 4.5 Security Management

The TOE can perform management functions specified in the Security Target. The administrator has full access to carry out all management functions, whereas the user will have limited privileges.

The TOE can also perform Bluetooth management functions. The TOE supports both Bluetooth BR/EDR and LE and uses Secure Simple Pairing (SSP) for security.

## 4.6 Protection of the TSF

The TOE implements the following protection of TSF data functions:

- Access controls
- Address space layout randomization (ASLR) with 16 bits of entropy
- Stack buffer overflow protection
- Verification of integrity of the bootchain and operating system executable code
- Trusted software updates using digital signatures

## 4.7 TOE Access

The TOE displays an advisory warning message regarding unauthorized use of the OS prior to establishment of a user session.

## 4.8 TOE Trusted Path/Channel

The TOE supports TLS 1.2 for trusted channel communications. The TOE uses TLS to securely communicate with the Apple Update Server. Applications may invoke the TOE-provided TLS to securely communicate with remote servers.

The TOE provides a trusted path between itself and local users that provides assured identification of its endpoints.

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.

# 5 Assumptions, Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the associated PPs:

- PP-Configuration for General Purpose Operating Systems and Bluetooth, Version 1.0, 2021-04-15; (CFG_GPOS-BT_V1.0)
    - Base PP: Protection Profile for General Purpose Operating Systems. Version 4.2.1, 2019-04-22, (PP_GPOS_V4.2.1)
    - PP Module: PP-Module for Bluetooth, Version 1.0, 2021-04-15, (MOD_BT_V1.0)

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.

## 5.1 Clarification of Scope

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

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 associated PPs) 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 guidance documentation was examined during the evaluation and must be used to configure, administer, and use the product in its evaluated configuration.

- Apple macOS 13 Ventura Common Criteria Configuration Guide, Version 1.1, dated 2024-01-12

Any additional documentation that was not included in the scope of evaluation should not be relied upon when configuring or operating the product as evaluated. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the product is configured as evaluated.

# 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 2.3.3 of the Assurance Activity Report (AAR).

## 7.1 Developer Testing

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

## 7.2 Evaluation Team Independent Testing

The ST lists more hardware platforms compared to the subset of platforms used for testing. Testing was performed on devices below:

- Mac mini (2020), M1 (Macmini9,1)
- MacBook Air (2022), M2 (Mac14,2)
- iMac Pro (2017), Skylake (iMacPro1,1)
- MacBook Air (2018), Amber Lake (MacBookAir8,1)
- MacBook Pro (2020), Ice Lake (MacBookPro16,2)
- MacBook Pro (2018), Coffee Lake (MacBookPro15,2)
- Mac Pro (2019), Cascade Lake (MacPro7,1)
- Mac mini (2023), M2 (Mac14,3)
- iMac (2020), Comet Lake (iMac20,2)

The list of test platforms is a subset of the list of platforms claimed in Appendix A.1 in [ST]. Although the claimed platforms differ in year produced and model, many are equivalent in terms of the components providing security functionality: CPU (with Secure Enclave Processor (SEP) hardware) and Bluetooth chip. They support the [PP_OS_v4.2.1] and [MOD_BT_v1.0] security functionality, respectively. These components are completely independent. For example, a Mac13,2 platform will provide the same [MOD_BT_v1.0] functionality as a Mac14,2 platform, even though the CPU microarchitecture is different. Similarly, a Mac14,2 platform will provide the same [PP_OS_v4.2.1] functionality as a Mac14,3 platform, even though the Bluetooth chip is different.

On Intel systems, the SEP is maintained as part of the T2 Security Chip, distinct from the general-purpose Intel SoC (System on a Chip). On the other hand, the SEP hardware is included in the Apple silicon SoCs.

Intel Core platforms include 4 microarchitectures: Ice Lake, Coffee Lake, Amber Lake, and Comet Lake. Intel Xeon W platforms include 2 microarchitectures: Cascade Lake and Skylake. Finally, the Apple silicon M1 and M2 platforms each includes 1 microarchitecture. The list of test platforms has at least one of each microarchitecture.

6 different Bluetooth chips are included in Appendix A.1 in [ST]. These chips are covered by the test platforms as follows:

- 4388: Mac14,3
- 4387: Mac14,2
- 4378: Macmini9,1
- 4377: MacBookPro16,2
- 4364: iMacPro1,1; MacBookPro15,2; MacPro7,1; iMac20,2
- 4355: MacBookAir8,1

Therefore, the selected subset of test platforms covers all unique combinations of the security-related components.

The basic testing infrastructure was configured as described in the evaluator test report. The TOE devices are connected to a private LAN network.

# 8 Evaluated Configuration

The guidance documentation provides specific instructions for configuring the TOE to comply with the functions defined in the Security Target. The evaluated configuration includes the devices listed in Appendix A.1 in [ST] running Apple macOS 13 Ventura.

# 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_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0) 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0) .

## 9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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 macOS 13 Ventura 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 that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit and the assurance activity specified in the CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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.

## 9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0), and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activity specified in the CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0), and that the conclusion reached by the evaluation team was justified.

## 9.5 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0), 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 and assurance activity specified in the CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0). 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 the TOE using the following sources. The search was performed on the following dates:

- 2023-05-08
- 2023-06-21
- 2023-07-25
- 2023-08-28
- 2023-09-21
- 2023-11-21
- 2024-01-09

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)
- Search US-Cert
- Google
- Apple Security Updates

The following search terms were used for CVE search on MITRE, NIST, and CISA web sites:

- macOS 13.2.1
- macOS corecrypto
- macOS common crypto
- macOS http
- macOS https
- macOS tls
- macOS tcp
- macOS ip
- macOS Bluetooth
- Apple silicon
- Apple M1
- Apple M1 Ultra
- Apple M1 Max

- Apple M1 Pro
- Apple M2
- Apple M2 Pro
- Apple M2 Max
- Apple T2
- Intel with T2
- Apple Secure Enclave
- Apple Security Enclave Processor
- Apple SEP
- Apple Lake
- Cascade Lake
- Coffee Lake
- Comet Lake
- Ice Lake
- Skylake
- ARM 8.5
- ARM 8.6
- Core i5-1030NG7
- Core i5-1038NG7
- Core i5-10500
- Core i5-10600
- Core i5-8210Y
- Core i5-8257U
- Core i5-8259U
- Core i5-8279U
- Core i5-8500
- Core i5-8500B
- Core i5-8557U
- Core i5-8600
- Core i5-9600K
- Core i7-1060NG7
- Core i7-1068NG7
- Core i7-10700K
- Core i7-8557U
- Core i7-8559U
- Core i7-8569U
- Core i7-8700
- Core i7-8700B
- Core i7-8750H
- Core i7-8850H
- Core i7-9750H
- Core i9-10910

- Core i9-8950HK
- Core i9-9880H
- Core i9-9900K
- Core i9-9980HK
- Xeon W-2140B
- Xeon W-2150B
- Xeon W-2170B
- Xeon W-2191B
- Xeon W-3223
- Xeon W-3235
- Xeon W-3245
- Xeon W-3265M
- Xeon W-3275M

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 Apple macOS 13 Ventura.

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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0), 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 performance of the testing defined by CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0) 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 CFG_GPOS-BT_V1.0 (PP_OS_v.4.2.1 and MOD_BT_v1.0), 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 documents listed in Section 6. No other 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 needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

Apple macOS 13 Ventura Security Target [ST] Version 1.1, dated 2024-01-12.

# 13 Glossary

The following definitions are used throughout this document.

| | |
|---|---|
| **ACL** | Access Control List |
| **AES** | Advanced Encryption Standard |
| **APFS** | Apple File System |
| **ARM** | Advanced RISC Machine |
| **ASLR** | Address Space Layout Randomization |
| **BR** | Basic Rate |
| **BSD** | Berkeley Software Distribution |
| **CBC** | Cipher Block Chaining |
| **CISA** | Cybersecurity and Infrastructure Agency |
| **CVE** | Common Vulnerability Database |
| **CC** | Common Criteria |
| **CCEVS** | Common Criteria Evaluation and Validation Scheme |
| **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 |
| **CVE** | Common Vulnerabilities and Exposures |
| **Conformance** | The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model. |
| **DRBG** | Deterministic Random Bit Generator |
| **EA** | Evaluation Activity |

| | |
|---|---|
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **EDR** | Enhanced Data Rate |
| **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. |
| **HMAC** | Keyed-hash Message Authentication Code |
| **ISA** | Instruction Set Architecture |
| **NIAP** | National Information Assurance Partnership |
| **NIST** | National Institute of Standards and Technology |
| **NSA** | National Security Agency |
| **NVD** | NIST National Vulnerability Database |
| **NVLAP** | National Voluntary Laboratory Assessment Program |
| **OE** | Operational Environment |
| **POSIX** | Portable Operating System Interface |
| **PP** | Protection Profile |
| **RSA** | Rivest-Shamir-Adleman |
| **SEP** | Secure Enclave Processor |
| **SHS** | Secure Hash Standard |
| **SoC** | System on a Chip |
| **SSP** | Secure Simple Pairing |
| **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. |
| **TSF** | TOE Security Functionality |
| **TLS** | Transport Layer 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. |
| **VPN** | Virtual Private Network |
| **VR** | Validation Report |
| **XNU** | X is Not Unix |

# 14 Bibliography

The validation 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
- Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
- PP-Configuration for General Purpose Operating Systems and Bluetooth, Version 1.0, April 15, 2021
- Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
- PP-Module for Bluetooth, Version 1.0, April 15, 2021
- Apple macOS 13 Ventura Common Criteria Configuration Guide, Version 1.1, January 12, 2024
- Apple macOS 13 Ventura Security Target Version 1.1, January 12, 2024
- Apple macOS 13 Ventura Assurance Activity Report, Version 1.1, January 12, 2024
- Evaluation Technical Report for a Target of Evaluation Apple macOS 13 Ventura, Version 1.1, January 12, 2024
- Apple macOS 13 Ventura Detailed Test Report, Version 1.1, January 8, 2024