National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Apple macOS 13 Ventura: FileVault

Report Number: CCEVS-VR-VID11348-2023
Dated: December 4, 2023
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D.
Jerome Myers, Ph.D.
Dave Thompson
The Aerospace Corporation

Common Criteria Testing Laboratory

King Ables
Alex Gong
Valerio Magliozzi
Stephan Mueller
Walker Riley
Joachim Vandersmissen
atsec information security corporation, Austin TX

Table of Contents

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Apple macOS 13 Ventura: FileVault on Apple silicon and T2 systems running macOS 13 Ventura provided by Apple Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied. 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 December 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Conformant and meets the assurance requirements given in:

- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.
- collaborative Protection Profile for Full Drive Encryption - Encryption Engine. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.

The TOE is Apple macOS 13 Ventura: FileVault.

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:

- [CPP_FDE_AA_V2.0E]: collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.
- [CPP_FDE_EE_V2.0E]: collaborative Protection Profile for Full Drive Encryption - Encryption Engine. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.

have been met.

The technical information included in this report was obtained from the Apple macOS 13 Ventura: FileVault Security Target, 11/28/2023 Version 1.1.

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, 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: FileVault
PP	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.

Item	Identifier
	collaborative Protection Profile for Full Drive Encryption - Encryption Engine. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.
ST	Apple macOS 13 Ventura: FileVault Security Target (ST), Version 1.1, dated 2023-11-28
ETR	Evaluation Technical Report for a Target of Evaluation Apple macOS 13 Ventura: FileVault, Version 1.1, dated 2023-11-29
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Apple Inc.
Developer	Apple Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Patrick Mallett, Jerome Myers, Dave Thompson

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: FileVault” full drive encryption product which supports an authorization acquisition and encryption engine. It is part of the macOS operating system. The macOS operating system is a Unix-based OS which leverages the Apple Secure Enclave, found in the Apple silicon System on a Chip (SoCs) and in the Apple T2 Security Chip, to perform full drive encryption. It also leverages an AES cryptographic implementation built in to the Direct Memory Access (DMA) controller chip. The operating system 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 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 Table 1.

Table 1: Devices Covered by the Evaluation

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
2023					
MacBook Pro (16-inch, 2023)	A2780	Mac14,6	M2 Max	ARMv8.6-A	SEP v2.0
		Mac14,10	M2 Pro	ARMv8.6-A	SEP v2.0
MacBook Pro (14-inch, 2023)	A2779	Mac14,5	M2 Max	ARMv8.6-A	SEP v2.0
		Mac14,9	M2 Pro	ARMv8.6-A	SEP v2.0
Mac mini (M2 Pro, 2023)	A2816	Mac14,12	M2 Pro	ARMv8.6-A	SEP v2.0
Mac mini (M2, 2023)	A2686	Mac14,3	M2	ARMv8.6-A	SEP v2.0
2022					
MacBook Pro (13-inch, M2, 2022)	A2338	Mac14,7	M2	ARMv8.6-A	SEP v2.0
MacBook Air (M2, 2022)	A2861	Mac14,2	M2	ARMv8.6-A	SEP v2.0
Mac Studio	A2615	Mac13,2	M1 Ultra	ARMv8.5-A	SEP v2.0
	A2615	Mac13,1	M1 Max	ARMv8.5-A	SEP v2.0
2021					
MacBook Pro (16-inch, 2021)	A2485	MacBookPro18,2	M1 Max	ARMv8.5-A	SEP v2.0
		MacBookPro18,1	M1 Pro	ARMv8.5-A	SEP v2.0
MacBook Pro (14-inch, 2021)	A2442	MacBookPro18,4	M1 Max	ARMv8.5-A	SEP v2.0
		MacBookPro18,3	M1 Pro	ARMv8.5-A	SEP v2.0
iMac (24-inch, M1, 2021)	A2438	iMac21,1	M1	ARMv8.5-A	SEP v2.0
	A2439	iMac21,2	M1	ARMv8.5-A	SEP v2.0
2020					
Mac mini (M1, 2020)	A2348	Macmini9,1	M1	ARMv8.5-A	SEP v2.0

Marketing Name	**Model #**	**Model Identifier**	**SoC/Processor**	**microArch**	**Security Chip**
MacBook Air (M1, 2020)	A2337	MacBookAir10,1	M1	ARMv8.5-A	SEP v2.0
MacBook Pro (13-inch, M1, 2020)	A2338	MacBookPro17,1	M1	ARMv8.5-A	SEP v2.0
MacBook Air (Retina, 13-inch, 2020)	A2179	MacBookAir9,1	Core i5-1030NG7 Core i7-1060NG7	Ice Lake	T2
MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	A2251	MacBookPro16,2	Core i5-1038NG7 Core i7-1068NG7	Ice Lake	T2
MacBook Pro (13-inch, 2020, Two Thunderbolt 3 ports)	A2289	MacBookPro16,3	Core i5-8257U Core i7-8557U	Coffee Lake	T2
iMac (Retina 5K, 27-inch, 2020)	A2115	iMac20,1 iMac20,2	Core i5-10500 Core i5-10600 Core i7-10700K Core i9-10910	Comet Lake	T2
2019					
MacBook Air (Retina, 13-inch, 2019)	A1932	MacBookAir8,2	Core i5-8210Y	Amber Lake	T2
MacBook Pro (13-inch, 2019, Four Thunderbolt 3 ports)	A1989	MacBookPro15,2	Core i5-8279U Core i7-8569U	Coffee Lake	T2
MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)	A2159	MacBookPro15,4	Core i5-8257U Core i7-8557U	Coffee Lake	T2
MacBook Pro (15-inch, 2019)	A1990	MacBookPro15,1 MacBookPro15,3	Core i7-9750H Core i9-9880H Core i9-9980HK	Coffee Lake	T2
MacBook Pro (16-inch, 2019)	A2141	MacBookPro16,1 MacBookPro16,4	Core i7-9750H Core i9-9880H Core i9-9980HK	Coffee Lake	T2

Marketing Name	Model #	Model Identifier	SoC/Processor	microArch	Security Chip
Mac Pro (2019)	A1991	MacPro7,1	Xeon W-3223 Xeon W-3235 Xeon W-3245 Xeon W-3265M Xeon W-3275M	Cascade Lake	T2
Mac Pro (2019 Rack)	A2304	MacPro7,1	Xeon W-3223 Xeon W-3235 Xeon W-3245 Xeon W-3265M Xeon W-3275M	Cascade Lake	T2
2018					
MacBook Air (Retina, 13-inch, 2018)	A1932	MacBookAir8,1	Core i5-8210Y	Amber Lake	T2
Mac mini (2018)	A1993	Macmini8,1	Core i5-8500B Core i7-8700B	Coffee Lake	T2
MacBook Pro (15-inch, 2018)	A1990	MacBookPro15,1 MacBookPro15,3	Core i7-8750H Core i7-8850H Core i9-8950HK	Coffee Lake	T2
MacBook Pro (13-inch, 2018, Four Thunderbolt 3 ports)	A1989	MacBookPro15,2	Core i5-8259U Core i7-8559U	Coffee Lake	T2
2017					
iMac Pro (2017)	A1862	iMacPro1,1	Xeon W-2140B Xeon W-2150B Xeon W-2170B Xeon W-2190B	Skylake	T2

3.2 Physical Scope of the TOE

The TOE includes both hardware and software running on the Macs listed in Appendix A.1 “Devices 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 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.

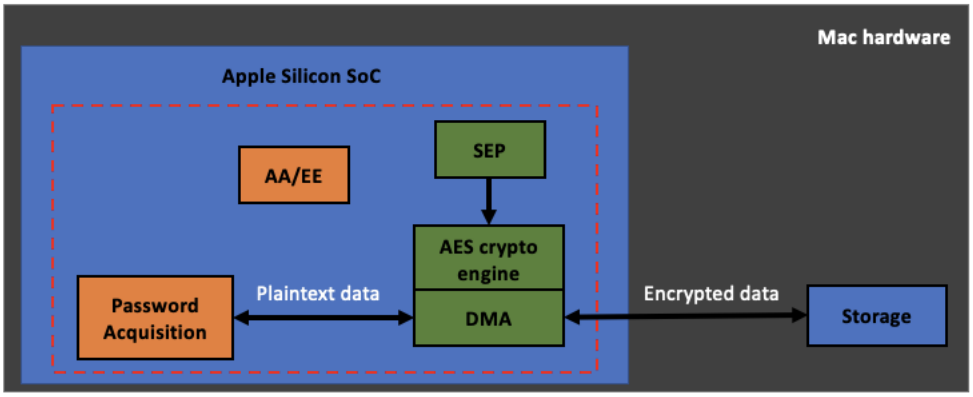
The TOE also includes the TOE documentation providing information for installing, configuring, and maintaining the evaluated configuration titled:

- Apple macOS 13 Ventura: FileVault Common Criteria Configuration Guide v1.0

Apple silicon

The Apple silicon SoC contains the Secure Enclave, which contains the Secure Enclave Processor (SEP) and runs the sepOS operating system, the application processor which runs macOS, and the DMA crypto engine. The Encryption Engine (EE) is instantiated in the Secure Enclave and the DMA crypto engine. The Acquisition component (AA) is instantiated in both the application processor (Password Acquisition) of the SoC and the Secure Enclave. The Secure Enclave provides security-related functionality for all the EE functionality (i.e., other than encryption/decryption of storage data) and all of the cryptographic functionality for AA (i.e., PBKDF2). The DMA crypto engine provides the AES implementation (a.k.a AES crypto engine) for encrypting and decrypting storage data. The AA is the pre-boot component on the storage drive and captures the user password and passes it to the Secure Enclave.

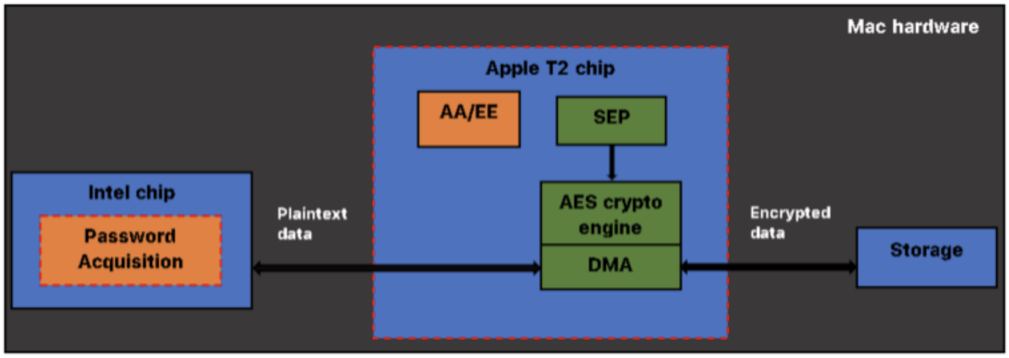
Figure 1: Apple silicon: Major components of TOE within red border



Intel with T2

The Apple T2 Security Chip runs the T2OS operating system and contains the Secure Enclave, which contains the Secure Enclave Processsor (SEP) and runs the sepOS operating system, and the DMA crypto engine. The Encryption Engine (EE) is instantiated on the T2. The AA is instantiated on both the Intel chip (Password Acquisition) and the T2. The T2 contains the Secure Enclave coprocessor which provides security-related functionality for all the EE functionality (i.e., other than encryption/decryption of storage data) and all of the cryptographic functionality for AA (i.e., PBKDF2). The AA is the pre-boot component on the disk and captures the user password and passes it to the SEP. The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the storage and main memory of the host platform.

Figure 2: Intel with T2: Major components of TOE within red border



The TOE also supports the following operational environmental component in the evaluated configuration.

- Apple Update Server to allow the TOE to download updates.

3.3 Un-evaluated Functionality

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

- Biometric Authentication – Many Apple Macs support biometric authentication. This feature is outside the scope of the evaluation.

4 Security Policy

4.1 Logical Scope of the TOE

The TOE implements the following security functions from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E].

4.2 Cryptographic Support

The TOE uses the following cryptographic modules to satisfy the cryptographic requirements defined in the ST:

- Apple silicon
    - Apple corecrypto Module 13.0 [Apple ARM, User, Software, SL1]
    - Apple corecrypto Module 13.0 [Apple ARM Kernel, Software, SL1]
    - Apple corecrypto Module 13.0 [Apple silicon, Secure Key Store, Hardware, SL2]
    - Apple DMA controller 2.0 [Hardware]
- Intel with T2

- Apple corecrypto Module 13.0 [Intel, User, Software, SL1]
- Apple corecrypto Module 13.0 [Intel, Kernel, Software, SL1]
- Apple corecrypto Module 13.0 [Apple ARM, Secure Key Store, Hardware, SL2]
- Apple DMA controller 1.0 [Hardware]

On Apple silicon Macs, the Apple corecrypto Module 13.0 [Apple ARM, User, Software, SL1] module resides in the macOS user space. The Apple corecrypto Module 13.0 [Apple ARM, Kernel, Software, SL1] module resides in the macOS kernel space. The Apple corecrypto Module 13.0 [Apple silicon, Secure Key Store, Hardware, SL2] module resides in the Secure Enclave. The Apple DMA controller 2.0 [Hardware] module resides in the DMA controller.

On "Intel with T2" Macs, the Apple corecrypto Module 13.0 [Intel, User, Software, SL1] module resides in the macOS user space. The Apple corecrypto Module 13.0 [Intel, Kernel, Software, SL1] module resides in the macOS kernel space. The Apple corecrypto Module 13.0 [Apple ARM, Secure Key Store, Hardware, SL2] module resides in the Secure Enclave. The Apple DMA controller 1.0 [Hardware] module resides in the DMA controller.

The table below lists the cryptographic algorithms claimed in this evaluation along with their respective standards.

Algorithms	Standards
AES	AES-CBC (as defined in NIST SP 800-38A)
AES	AES-KW (AES as specified in ISO/IEC 18033-3, [NIST SP 800-38F]
AES	AES-XTS (AES as specified in ISO/IEC 18033-3 and XTS as specified in IEEE 1619)
ECDSA	FIPS PUB 186-4 Digital Signature Standard (DSS), Section 6 and Appendix D
RSA	FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3
HMAC	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”
SHS	NIST FIPS Pub 180-4
DRBG	CTR_DRBG (AES)

4.3 User Data Protection

The TOE encrypts all user data using the following algorithms:

- Apple silicon: AES-XTS-256 using two independent 256-bit keys

- Intel with T2: AES-XTS-128 using two independent 128-bit keys

When the host platform is provisioned at first run, the user is prompted to enable the TOE's embedded FDE encryption management program (FileVault) and enter a username and password. Once enabled, the storage drive of the host platform remains encrypted and protected from unauthorized access; even if the physical storage device is removed and connected to another host platform.

4.4 Security Management

The TOE can perform management functions. The administrator has full access to carry out all management functions, and the user has limited privilege. The System Settings >> Privacy & Security menu on macOS invokes management functionality of the Authorization Acquisition component which supports forwarding requests to change or cryptographically erase the Data Encryption Key (DEK) to the Encryption Engine component as well as configuring authorization factors. The Authorization Acquisition and Encryption Engine components together supports user initialization of the TOE firmware/software updates.

4.5 Protection of the TSF

The TOE implements the following protection of TSF data:

- Protection of key and key material—The TOE only stores keys in non-volatile memory when cryptographically wrapped.
- Power saving states and timing of power states—The TOE supports G2(S5) (Soft Off (Shutdown)) state as well as allowing the user to initiate the power saving state.
- TSF Testing—The TOE performs Known Answer Tests (KATs) to verify the correct operation of supported cryptographic functions.
- Trusted updates—Before installing the updates, the TOE’s Authorization Acquisition component validates the digital signature of the updates retrieved by the macOS operating system from the Apple Update Server.

5 Assumptions, Clarification of Scope

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

- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.
- collaborative Protection Profile for Full Drive Encryption - Encryption Engine. Version 2.0 + Errata 20190201 as of 2019-02-01; exact conformance.

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 to be performed by the evaluation team).

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

6 Documentation

The following documentation was used as evidence for the evaluation of the TOE.

Reference	Document Name	Location
[CCGuide]	Apple macOS 13 Ventura: FileVault Common Criteria Configuration Guide v1.1	https://www.niap-ccevs.org/MMO/Product/st_vid11348-agd.pdf

Any additional customer documentation delivered with the product or that may be available through download was not included in the scope of the evaluation and, hence, should not be relied upon when configuring or using the products in the evaluated configuration.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

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 specific test configurations and test tools utilized may be found in the AAR Section 2.3.3.

The ST lists more hardware platforms compared to the subset of platforms used for testing.

The ST provides a rationale that the tested platforms adequately represent the listed platforms. Testing was performed on devices below:

- Intel Xeon W iMac Pro (iMacPro1,1)
- M1 Mac mini (Macmini9,1)
- M2 Mac mini (Mac14,3)

The ST defines security functions which are provided by the Secure Enclave Processor (SEP) that is present in the different TOE hardware systems. On Intel systems, the SEP is maintained as part of the T2 Security Chip. As all Intel systems use the same T2 chip, the SEP hardware is identical for all these systems. This leads to the conclusion that the test results obtained on one T2 chip are equally applicable to all other T2 chip use cases. Therefore, testing on one Intel system with a T2 chip is considered to cover all other Intel systems with T2 chips.

For the Apple silicon systems M1 and M2, testing is conducted separately from the Intel systems. Testing platforms are selected by choosing an ISA (instruction set architecture) from each SoC (System on a Chip) family. All M1 systems have the same ARMv8.5-A ISA and all M2 systems have same ARMv8.6-A ISA. All Apple silicon SoC's contain the Secure Enclave Processor (SEP) which similarly provides the security functions defined in the ST. Therefore, testing one ISA per SoC is considered sufficient.

The test systems were set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing. The basic testing infrastructure was configured by connecting the TOE devices 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.

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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 conformant and to meet the assurance requirements defined by the [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E].

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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: FileVault products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the Apple macOS 13 Ventura: FileVault 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. 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 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 evaluation team used the following search terms, as described in the PPs:

- Apple macOS 13 Ventura: FileVault
- macos Ventura 13
- AES used in XTS mode
- single overwrite zeroization
- Apple corecrypto Module 13.0 (Software and Hardware)
- Apple silicon
- Intel with T2
- Secure Enclave
- 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 searches were performed on multiple occasions between:

- 2023-05-08 and 2023-05-12
- 2023-05-18 and 2023-05-22
- 2023-09-29 and 2023-10-23
- 2023-10-25 and 2023-10-26
- 2023-11-02 and 2023-11-28

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 releases of macOS 13 prior to the evaluated version.

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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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

[CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] 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 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

Validation Report for Apple macOS 13 Ventura: FileVault Security Target (ST) Version 1.1, dated 2023-11-28

13 Glossary

The following definitions are used throughout this document.

AA	Authorization Acquisition
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
CBC	Cipher Block Chaining
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
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DMA	Direct Memory Access
DSS	Digital Signature Standard
EA	Evaluation Activity
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	Encryption Engine
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.
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
G2(S5)	Soft Off (Shutdown) state
HMAC	Keyed-hash Message Authentication Code
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
ISA	Instruction Set Architecture
ISO	International Organization or Standardization
KAT	Known Answer Test
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PBKDF2	Password Based Key Derivation Function 2
PP	Protection Profile
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SEP	Secure Enclave Processor
SFR	Security Functional Requirement
SHS	Secure Hash Standard
SoC	System on a Chip
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
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.
VR	Validation Report
XNU	X is Not Unix
XTS	XEX Tweakable Block Ciphertext Stealing

14 Bibliography

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

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017
- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201 as of 2019-02-01
- collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201 as of 2019-02-01
- Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition February 2019, Version 2.0 + Errata 20190201
- Supporting Document Mandatory Technical Document Full Drive Encryption: Encryption Engine February 2019, Version 2.0 + Errata 20190201
- Apple macOS 13 Ventura: FileVault Common Criteria Configuration Guide, Version 1.1, 2023-11-28
- Apple macOS 13 Ventura: FileVault Security Target Version 1.1, 2023-11-28
- Apple macOS 13 Ventura: FileVault Assurance Activity Report, Version 1.1, 2023-11-29