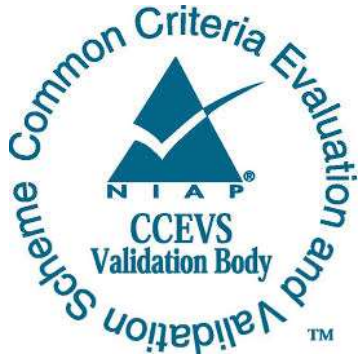
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Apple macOS 14 Sonoma: FileVault

Report Number:	CCEVS-VR-VID11448-2025
Dated:	May 14, 2025
Version:	1.0

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

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

Acknowledgements

Validation Team

Patrick Mallett, Ph.D.

Jerome Myers, Ph.D.

Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Joachim Vandersmissen

Amr Said

Hunter Barton

Walker Riley

atsec information security corporation

Austin, TX

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Apple macOS 14 Sonoma: FileVault (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

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

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

2 Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple macOS 14 Sonoma: FileVault running on the Apple devices listed in **Table *3***.
Security Target	Apple macOS 14 Sonoma: FileVault Security Target, Version 1.2, 2025-05-08

Sponsor & Developer	Apple Inc.
Completion Date	May 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	PP Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0. This PP-Configuration is comprised of the following components: • collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201 • collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Evaluation Personnel	Joachim Vandersmissen, Amr Said, Hunter Barton, Walker Riley
Validation Personnel	Patrick Mallett, Ph.D., Jerome Myers, Ph.D., Mike Quintos

3 TOE Architecture

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

The TOE is Apple macOS 14 Sonoma: FileVault, which is a Full Drive Encryption (FDE) solution including both Authorization Acquisition (AA) and Encryption Engine (EE) components. The TOE is a built-in security feature providing data-at-rest protection on Apple Mac computers. It is a hybrid FDE implementation based on a single vendor's combination of hardware and software.

The Mac computers run Apple macOS operating system. Apple macOS is a POSIX-compliant operating system (OS) built on top of the XNU kernel. The TOE is part of the macOS operating system which leverages the Apple silicon System on Chip (SoC) or the Apple T2 Security Chip. Included in the Apple silicon SoC and the Apple T2 Security Chip are Apple Secure Enclave and DMA Storage Controller. The Secure Enclave is a dedicated secure subsystem where all FDE cryptographic key handling occurs. The DMA Storage Controller provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the storage and main memory, making data encryption with AES-XTS efficient. A special channel from the Secure Enclave securely transfers necessary keying material to the AES engine.

The tested version of the TOE is Apple macOS 14.2.1.

The TOE includes both hardware and software running on the Mac computers listed in **Table 3**. These Mac computers are organized into the following two groups:

- Apple silicon Mac computers
- "Intel with T2" Mac computers

The Apple silicon SoC includes:

- the application processor, which is the main processor of the TOE device and runs the macOS operating system;
- the Secure Enclave, which contains the Secure Enclave Processor (SEP) running the sepOS operating system; and
- the DMA Storage Controller, which performs the storage encryption

The EE component is instantiated in the Secure Enclave and the DMA Storage Controller. The AA component is instantiated in the application processor (Password Acquisition) and the Secure Enclave. The Secure Enclave provides security related functionality for EE (other than encryption/decryption of storage data), as well as all of the cryptographic functionality for AA (i.e., PBKDF2). The DMA Storage Controller provides a dedicated AES crypto engine built into the DMA path between storage and main memory of the host platform. The Password Acquisition function of AA component is implemented as the pre-boot component on the storage drive. It captures the user password and passes it to the Secure Enclave.

Intel with T2 includes:

- the application processor, which is the co-processor to the Intel processor and runs T2OS operating system; the Intel processor is the main processor running macOS;
- the Secure Enclave, which contains the SEP running the sepOS operating system; and
- the DMA Storage Controller, which performs the storage encryption.

The EE component is instantiated on the T2. The AA component is instantiated on both the Intel processor (Password Acquisition) and the T2. The Secure Enclave provides security related functionality for EE (other than encryption/decryption of storage data), as well as all of the cryptographic functionality for AA (i.e., PBKDF2). The DMA Storage Controller provides a dedicated AES crypto engine built into the DMA path between the storage and main memory of the host platform. The Password Acquisition function of AA component is implemented as the pre-boot component on the storage drive. It captures the user password and passes it to the Secure Enclave.

4 Environmental Strengths

The TOE provides the following security functions as described in the ST.

4.1 Cryptographic Support

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

- Apple silicon
  - Apple corecrypto Module v14.0 [Apple silicon, User, Software, SL1]
  - Apple corecrypto Module v14.0 [Apple silicon, Kernel, Software, SL1]
  - Apple corecrypto Module v14.0 [Apple silicon, Secure Key Store, Hardware, SL2]
  - Apple DMA Storage Controller v2.0 [Hardware]
- Intel with T2
  - Apple corecrypto Module v14.0 [Intel, User, Software, SL1]
  - Apple corecrypto Module v14.0 [Intel, Kernel, Software, SL1]

- Apple corecrypto Module v14.0 [Intel, Secure Key Store, Hardware, SL2]
- Apple DMA Storage Controller v1.0 [Hardware]

The evaluation supports the following cryptographic algorithms along with their respective standards.

Table 2: Cryptographic algorithms

Algorithms	Standards
AES-CBC	NIST SP 800-38A
AES-KW	NIST SP 800-38F
AES-XTS	NIST SP 800-38E
ECDSA	FIPS 186-4
RSA	FIPS 186-4
HMAC	FIPS 198-1
SHA	FIPS 180-4
CTR_DRBG (AES)	NIST SP 800-90A Rev. 1

4.2 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

4.3 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. The Authorization Acquisition and Encryption Engine components together supports user initiation of the TOE firmware/software updates.

4.4 Protection of TSF

The TOE implements the following protection of TSF functions and data:

- Protection of key and key material—The TOE only stores keys in non-volatile memory when wrapped and plaintext keys are not part of the supported key bags.
- Power saving states and timing of power states—The TOE supports G2(S5) state and allows the user to initiate this 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 and Clarification of Scope

5.1 Assumptions

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

5.2 Clarification of Scope

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

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Apple macOS 14 Sonoma: FileVault ([ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The following guidance documentation was examined during the evaluation:

- Apple macOS 14 Sonoma: FileVault Common Criteria Configuration Guide, Version 1.0, 2025-04-10 ([CCGUIDE])

Only the Administrator Guide listed above and the specified sections of the other documents reference by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

7 IT Product Testing

This section describes the testing efforts of the evaluation team.

A non-proprietary description of the tests performed, and their results is provided in the Assurance Activity Report ([AAR]). A description of the test environment and a list of tools used for testing is provided in Section 2.3.4 of the AAR.

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

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

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

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

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

7.1 Test Configuration

The evaluation team established a test configuration comprising Apple macOS 14 Sonoma: FileVault running on the Apple Mac devices listed below. The Assurance Activities Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE.

- MacBook Pro (2020), Ice Lake (MacBookPro16,2)
- Mac mini (2020), M1 (Macmini9,1)
- Mac mini (2023), M2 (Mac14,3)
- MacBook Pro (2023), M3 Max (Mac15,8)

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of hardware and software, when configured in according with the documentation specified in Section 6. The evaluation covers Apple macOS 14 Sonoma: FileVault running on the Apple Mac devices listed below.

Table 3: Mac Devices Covered by the Evaluation

Marketing Name	Model #	Model Identifier	SoC/Processor	MicroArch	SEP core
2023					
MacBook Pro (14-inch, Nov 2023)	A2992	Mac15,10 Mac15,8	M3 Max	ARMv8.6-A	Built-in
		Mac15,6	M3 Pro	ARMv8.6-A	Built-in
	A2918	Mac15,3	M3	ARMv8.6-A	Built-in
MacBook Pro (16-inch, Nov 2023)	A2991	Mac15,11 Mac15,9	M3 Max	ARMv8.6-A	Built-in
		Mac15,7	M3 Pro	ARMv8.6-A	Built-in
iMac (24-inch, 2023, Two ports)	A2784	Mac15,4	M3	ARMv8.6-A	Built-in
iMac (24-inch, 2023, Four ports)	A2783	Mac15,5	M3	ARMv8.6-A	Built-in
Mac Studio (2023)	A2901	Mac14,14	M2 Ultra	ARMv8.6-A	Built-in
		Mac14,13	M2 Max	ARMv8.6-A	Built-in
Mac Pro (2023)	A2786	Mac14,8	M2 Ultra	ARMv8.6-A	Built-in
Mac Pro (Rack, 2023)	A2787	Mac14,8	M2 Ultra	ARMv8.6-A	Built-in
MacBook Air (15-inch, M2, 2023)	A2941	Mac14,15	M2	ARMv8.6-A	Built-in

Marketing Name	Model #	Model Identifier	SoC/Processor	MicroArch	SEP core
MacBook Pro (16-inch, 2023)	A2780	Mac14,6	M2 Max	ARMv8.6-A	Built-in
		Mac14,10	M2 Pro	ARMv8.6-A	Built-in
MacBook Pro (14-inch, 2023)	A2779	Mac14,5	M2 Max	ARMv8.6-A	Built-in
		Mac14,9	M2 Pro	ARMv8.6-A	Built-in
Mac mini (M2 Pro, 2023)	A2816	Mac14,12	M2 Pro	ARMv8.6-A	Built-in
Mac mini (M2, 2023)	A2686	Mac14,3	M2	ARMv8.6-A	Built-in
2022					
MacBook Pro (13-inch, M2, 2022)	A2338	Mac14,7	M2	ARMv8.6-A	Built-in
MacBook Air (M2, 2022)	A2861	Mac14,2	M2	ARMv8.6-A	Built-in
Mac Studio (2022)	A2615	Mac13,2	M1 Ultra	ARMv8.5-A	Built-in
		Mac13,1	M1 Max	ARMv8.5-A	Built-in
2021					
MacBook Pro (16-inch, 2021)	A2485	MacBookPro18,2	M1 Max	ARMv8.5-A	Built-in
		MacBookPro18,1	M1 Pro	ARMv8.5-A	Built-in
MacBook Pro (14-inch, 2021)	A2442	MacBookPro18,4	M1 Max	ARMv8.5-A	Built-in
		MacBookPro18,3	M1 Pro	ARMv8.5-A	Built-in
iMac (24-inch, M1, 2021)	A2438	iMac21,1	M1	ARMv8.5-A	Built-in
	A2439	iMac21,2	M1	ARMv8.5-A	Built-in
2020					
Mac mini (M1, 2020)	A2348	Macmini9,1	M1	ARMv8.5-A	Built-in
MacBook Air (M1, 2020)	A2337	MacBookAir10,1	M1	ARMv8.5-A	Built-in
MacBook Pro (13-inch, M1, 2020)	A2338	MacBookPro17,1	M1	ARMv8.5-A	Built-in
MacBook Air (Retina, 13-inch, 2020)	A2179	MacBookAir9,1	Core i7-1060NG7	Ice Lake	T2 chip
MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	A2251	MacBookPro16,2	Core i7-1068NG7	Ice Lake	T2 chip
MacBook Pro (13-inch, 2020, Two Thunderbolt 3 ports)	A2289	MacBookPro16,3	Core i5-8257U Core i7-8557U	Coffee Lake	T2 chip
iMac (Retina 5K, 27-inch, 2020)	A2115	iMac20,1	Core i5-10500 Core i5-10600 Core i7-10700K Core i9-10910	Comet Lake	T2 chip
		iMac20,2	Core i7-10700K Core i9-10910	Comet Lake	T2 chip
2019					
MacBook Air (Retina, 13-inch, 2019)	A1932	MacBookAir8,2	Core i5-8210Y	Amber Lake	T2 chip

Marketing Name	Model #	Model Identifier	SoC/Processor	MicroArch	SEP core
MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)	A2159	MacBookPro15,4	Core i5-8257U Core i7-8557U	Coffee Lake	T2 chip
MacBook Pro (16-inch, 2019)	A2141	MacBookPro16,1 MacBookPro16,4	Core i7-9750H Core i9-9880H Core i9-9980HK	Coffee Lake	T2 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 chip
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 chip

8.2 Excluded Functionality

The following product functionalities are not included in the CC evaluation:

- General Purpose Operating System functionality – The TOE is an integral part of Apple macOS 14 Sonoma; however, the evaluation is limited to the FDE functionality.
- Disk unlocking using an iCloud account.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Apple macOS 14 Sonoma: FileVault ([ETR]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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

The evaluation determined the TOE satisfies the conformance claims made in the [ST], which is CC Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in the *PPs* listed in **Table 1**.

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

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

The evaluation team performed each TSS assurance activity and each work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, and ASE_TSS.1 CEM. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements

claimed to be met by the product that are consistent with the claimed *PPs* and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development Activities (ADV)

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

9.3 Evaluation of the Guidance Activities (AGD)

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

9.6 Vulnerability Assessment Activity (AVA)

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

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

- Apple security releases
  - https://support.apple.com/en-us/100100
- MITRE Common Vulnerabilities and Exposures (CVE) List:
  - https://cve.mitre.org/cve/search_cve_list.html
- National Vulnerability Database:
  - https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities Catalog:
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches throughout the evaluation process, in particularly using the following search terms as described in the Protection Profiles:

- Apple macOS 14 Sonoma: FileVault
- macOS Sonoma 14
- AES used in XTS mode
- Apple corecrypto Module 14.0
- Apple silicon
- Intel with T2
- Secure Enclave
- ARMv8.5-A, ARMv8.6-A
- Ice Lake, Coffee Lake, Comet Lake, Amber Lake, Coffee Lake, Cascade Lake
- Core i7-1060NG7, Core i7-1068NG7, Core i5-8257U, Core i7-8557U, Core i5-10500, Core i5-10600, Core i7-10700K, Core i9-10910, Core i5-8210Y, Core i5-8257U, Core i7-8557U, Core i7-9750H, Core i9-9880H, Core i9-9980HK
- Xeon W-3223, Xeon W-3235, Xeon W-3245, Xeon W-3265M, Xeon W-3275M, Xeon W-3223, Xeon W-3235, Xeon W-3245, Xeon W-3265M, Xeon W-3275M
- M3, M2, M1

The most recent search was performed on 2025-05-09 and the results did not identify any vulnerabilities that are applicable to the security functionality of the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

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

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the guidance documents listed in Section 6 of this report. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product were not assessed as part of this evaluation and no further conclusions can be drawn about their effectiveness. No other versions of the TOE, either earlier or later, were evaluated.

All other items and scope issues have been sufficiently addressed in other sections of this document.

11 Security Target

The ST for this product's evaluation is Apple macOS 14 Sonoma: FileVault Security Target, Version 1.2, 2025-05-08 ([ST]).

A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

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

B Bibliography

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

[CCPART1]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
[CCPART2]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
[CCPART3]	Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
[CEM]	Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
[CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0]	Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0, 2024-05-31
[CPP_FDE_AA_V2.0E]	collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, 2019-02-01
[CPP_FDE_EE_V2.0E]	collaborative Protection Profile for Full Drive Encryption Encryption Engine, Version 2.0 + Errata 20190201, 2019-02-01
[AAR]	Assurance Activity Report Apple macOS 14 Sonoma: FileVault, Version 1.1, 2025-05-09
[ETR]	Evaluation Technical Report Apple macOS 14 Sonoma: FileVault, Version 1.1, 2025-05-09
[CCGUIDE]	Apple macOS 14 Sonoma: FileVault Common Criteria Configuration Guide, Version 1.0, 2025-04-10
[ST]	Apple macOS 14 Sonoma: FileVault Security Target, Version 1.2, 2025-05-08