National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report for

Apple macOS 26 Tahoe: FileVault

Report Number:	CCEVS-VR-VID11696-2026
Dated:	July 29, 2026
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

Mike Quintos

Jerome Myers, Ph. D.

Patrick Mallett, Ph. D.

The Aerospace Corporation

Common Criteria Testing Laboratory

Joachim Vandersmissen

Evan Barnett

James Reid

Parker Collier

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 26 Tahoe: FileVault, the Target of Evaluation (TOE). The TOE is a Full Drive Encryption (FDE) solution developed by Apple Inc. that includes 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, comprising both hardware elements (Apple silicon System on Chip including Secure Enclave and DMA Storage Controller) and software (macOS Tahoe 26.3 operating system components). 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.

The evaluation was performed by atsec information security corporation Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed on July 29, 2026. The Certification/Validation Identification is CCEVS-VR-VID11696-2026.

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 PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0), which includes:

- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201 (CPP_FDE_AA_V2.0E)
- collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201 (CPP_FDE_EE_V2.0E)

The TOE provides comprehensive data-at-rest protection through full drive encryption using AES-XTS-256. Key security functions include: cryptographic support via Apple corecrypto version 26 and hardware-based cryptographic operations; user data protection encrypting all data with AES-XTS-256; security management capabilities for administrators and users; and protection of TSF data including key material protection, secure power states, cryptographic self-tests, and trusted software updates with digital signatures.

The TOE addresses threats related to unauthorized access to encrypted data at rest, unauthorized disclosure of sensitive information through physical access to storage media, and compromise of cryptographic key material.

The TOE must be installed, configured, and managed strictly in accordance with the Apple macOS 26 Tahoe: FileVault Common Criteria Guide, Version 1.0, 2026-06-29. The evaluated configuration covers Apple macOS 26 Tahoe: FileVault running on specific Apple Mac devices with Apple silicon (M2, M3, M4, and M5 Series processors) as enumerated in Table 2 of this report. Consumers should download the configuration guide from the NIAP website to ensure proper evaluated configuration.

The evaluation assumes that the TOE will be used in accordance with the assumptions specified in the claimed Protection Profiles, including that the operational environment provides physical security commensurate with the value of the TOE and the data it protects, and that administrators are non-hostile, appropriately trained, and follow all administrator guidance.

This VR applies only to the specific version and configuration of the product as evaluated and documented in the Security Target. The evaluation covered only the specific software distribution and version identified (macOS Tahoe 26.3), not any earlier or later versions. The evaluation of security functionality was limited to the functionality specified in the Security Target; excluded functionality includes General Purpose Operating System functionality and disk unlocking using an iCloud account.

This VR is intended to assist end users and security certification agents in determining the suitability of this Information Technology (IT) product in their environment. End users should review the Security Target, which

contains specific security claims, in conjunction with this VR, which describes how those claims were evaluated and tested. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the validator comments in Section 10, where restrictions on the evaluated configuration are highlighted. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports written by atsec.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The Common Criteria Evaluation and Validation Scheme (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/PP-Modules/Packages to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Validation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Apple macOS 26 Tahoe: FileVault
Security Target	Apple macOS 26 Tahoe: FileVault Security Target, Version 1.1, 2026-06-29
Sponsor & Developer	Apple Inc.
Completion Date	July 29, 2026
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 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0) • collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201 (CPP_FDE_AA_V2.0E) • collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201 (CPP_FDE_EE_V2.0E)
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
Validation Personnel	Mike Quintos, Jerome Myers, Patrick Mallett
Evaluation Personnel	Joachim Vandersmissen, Evan Barnett, James Reid, Parker Collier, Walker Riley

3 TOE Architecture

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

The TOE is Apple macOS 26 Tahoe: 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 with Apple silicon. 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. The TOE is part of the macOS operating system, which leverages the Apple silicon System on Chip (SoC). Included in the Apple silicon SoC are Apple Secure Enclave and Direct Memory Access (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-XTS crypto engine built into the 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-XTS engine.

The macOS version used in evaluation testing is 26.3.

The TOE includes both hardware and software running on the Mac computers listed in Table 2.

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 (Login Window) 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 and AES-CBC). The DMA Storage Controller provides a dedicated AES-XTS crypto engine built into the DMA path between storage and main memory of the host platform. The Login Window of the 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 includes version 26 of the Apple corecrypto cryptographic implementations and is supported by the onboard Apple Secure Enclave hardware for performing user space, kernel space, and Secure Enclave cryptographic operations. In addition, it uses a hardware-based noise source for entropy generation. The Apple DMA Storage Controller hardware implements the AES-XTS cryptographic algorithm supported for data-at-rest encryption.

4.2 User Data Protection

The TOE encrypts all user data using AES-XTS-256.

4.3 Security Management

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

4.4 Protection of the TSF

The TOE implements the following protection of TOE Security Functionality (TSF) data:

- Protection of keys and key material.
- Compliant power saving states that purge security-relevant data upon entry.
- Cryptographic self-tests at start-up of the TOE.
- Trusted software updates using digital signatures.

The macOS operating system retrieves the update package from the Apple Update Server and forwards the package to the AA component. The TOE validates the digital certificate for the package before it is installed.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PPs, PP-Modules, and Packages to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, PP-Modules, and Packages, 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, PP-Modules, and Packages specified in Table 1.

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in the [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 vendor provides guidance documents describing the installation process for Apple macOS 26 Tahoe: FileVault, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

- Apple macOS 26 Tahoe: FileVault Common Criteria Guide, Version 1.0, 2026-06-29 (CCGUIDE)

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website. Only the guidance documentation listed above and the specified sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of the TOE in its evaluated configuration. Any other documentation (e.g., published on the vendor's website) was not covered by the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated.

7 IT Product Testing

The test plan, procedures, and evidence are documented in the proprietary Detailed Test Report ([DTR]). A non-proprietary description of the tests performed, and their results is provided in the Assurance Activity Report ([AAR]).

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

7.1 Developer Testing

No evidence of developer testing is required by the assurance activities for this TOE.

7.2 Evaluation Team Testing

The evaluation team established a test configuration comprising Apple macOS 26 Tahoe: FileVault running on the platforms listed below.

- MacBook Air (Mac14,2)
- MacBook Pro (Mac15,8)
- MacBook Pro (Mac16,8)
- MacBook Pro (Mac17,2)

Section 2.3.5 of the Assurance Activity Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

The evaluation team devised a Test Plan based on the Test Activities specified in the above PPs. 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 Apple facility in Cupertino, CA from February 2026 to March 2026.

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.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured in accordance with the documentation specified in Section 6. The evaluation covers Apple macOS 26 Tahoe: FileVault running on the Apple Mac devices listed below.

Table 2: Mac Devices Covered by the Evaluation

Marketing Name	Model Identifier	Processor (Micro Architecture)	Security Chip
MacBook Pro (14-inch, M5)	Mac17,2	M5 (ARMv9.3-A)	SEP v3.0
MacBook Air (15-inch, M4, 2025)	Mac16,13	M4 (ARMv9.2-A)	SEP v2.0
MacBook Air (13-inch, M4, 2025)	Mac16,12	M4 (ARMv9.2-A)	SEP v2.0
Mac Studio (2025)	Mac16,9	M4 Max (ARMv9.2-A)	SEP v2.0
Mac Studio (2025)	Mac15,14	M3 Ultra (ARMv8.6-A)	SEP v2.0
MacBook Pro (14-inch, 2024)	Mac16,8	M4 Pro (ARMv9.2-A)	SEP v2.0
	Mac16,6	M4 Max (ARMv9.2-A)	SEP v2.0
	Mac16,1	M4 (ARMv9.2-A)	SEP v2.0
MacBook Pro (16-inch, 2024)	Mac16,7	M4 Pro (ARMv9.2-A)	SEP v2.0
	Mac16,5	M4 Max (ARMv9.2-A)	SEP v2.0
iMac (24-inch, 2024, Two ports)	Mac16,3	M4 (ARMv9.2-A)	SEP v2.0
	Mac16,2	M4 (ARMv9.2-A)	SEP v2.0
Mac mini (2024)	Mac16,11	M4 Pro (ARMv9.2-A)	SEP v2.0
	Mac16,10	M4 (ARMv9.2-A)	SEP v2.0
MacBook Air (15-inch, M3, 2024)	Mac15,13	M3 (ARMv8.6-A)	SEP v2.0
MacBook Air (13-inch, M3, 2024)	Mac15,12	M3 (ARMv8.6-A)	SEP v2.0
MacBook Pro (14-inch, Nov 2023)	Mac15,10	M3 Max (ARMv8.6-A)	SEP v2.0
	Mac15,8	M3 Max (ARMv8.6-A)	SEP v2.0
	Mac15,6	M3 Pro (ARMv8.6-A)	SEP v2.0
	Mac15,3	M3 (ARMv8.6-A)	SEP v2.0
MacBook Pro (16-inch, Nov 2023)	Mac15,11	M3 Max (ARMv8.6-A)	SEP v2.0

	Mac15,9	M3 Max (ARMv8.6-A)	SEP v2.0
	Mac15,7	M3 Pro (ARMv8.6-A)	SEP v2.0
iMac (24-inch, 2023, Four ports)	Mac15,5	M3 (ARMv8.6-A)	SEP v2.0
iMac (24-inch, 2023, Two ports)	Mac15,4	M3 (ARMv8.6-A)	SEP v2.0
Mac Pro (-/Rack 2023)	Mac14,8	M2 Ultra (ARMv8.6-A)	SEP v2.0
MacBook Air (15-inch, 2023)	Mac14,15	M2 (ARMv8.6-A)	SEP v2.0
Mac Studio (2023)	Mac14,14	M2 Ultra (ARMv8.6-A)	SEP v2.0
	Mac14,13	M2 Max (ARMv8.6-A)	SEP v2.0
MacBook Pro (16-inch, 2023)	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)	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)	Mac14,12	M2 Pro (ARMv8.6-A)	SEP v2.0
Mac mini (M2, 2023)	Mac14,3	M2 (ARMv8.6-A)	SEP v2.0
MacBook Pro (13-inch, M2, 2022)	Mac14,7	M2 (ARMv8.6-A)	SEP v2.0
MacBook Air (M2, 2022)	Mac14,2	M2 (ARMv8.6-A)	SEP v2.0

8.2 Excluded Functionality

- General Purpose Operating System functionality. The TOE is partially implemented in the Apple macOS operating system; however, the evaluation is limited to the FDE functionality. General Purpose Operating System functionality is not part of this evaluation.
- 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 26 Tahoe: 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, PP-Modules, and Packages listed in Table 1.

The evaluation determined the TOE satisfies the conformance claims made in the Apple macOS 26 Tahoe: FileVault Security Target, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in the PPs, PP-Modules, and Packages listed in Table 1.

The validation team 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 were justified.

9.1 Evaluation of the Development Activities (ADV)

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

9.2 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each CEM work unit from AGD_OPE.1 and AGD_PRE.1. 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.

9.3 Evaluation of the Life Cycle Support Activities (ALC)

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

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

The evaluation team performed each TSS assurance activity and each CEM 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. 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, PP-Modules, and Packages, and security function descriptions that satisfy the requirements.

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

The evaluation team performed each ATE assurance activity and applied each CEM work unit from ATE_IND.1. The evaluation team ran the set of tests specified by the claimed PPs, PP-Modules, and Packages and recorded the results in the Test Report, summarized in section 2.3.5 of the [AAR].

9.6 Evaluation of the Vulnerability Assessment Activity (AVA)

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

The following search terms were used during the vulnerability search:

- FileVault
- macOS 26
- Secure Enclave Processor
- corecrypto
- AES-XTS
- single overwrite zeroization
- Apple M2
- Apple M3
- Apple M4
- Apple M5

The evaluator searched for publicly known vulnerabilities using the following sources:

- MITRE Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- CISA Known Exploited Vulnerabilities (KEV) Catalog
- Apple security releases: https://support.apple.com/en-us/100100
- Background Security Improvements by date: https://support.apple.com/en-us/111333

The vulnerability search was repeated on the following dates, throughout the evaluation process: 2026-06-29 and 2026-07-28. All “crucial” and non-crucial vulnerabilities (as defined by the NIAP Policy 17 Addendum) found during the vulnerability search were mitigated. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist in the TOE.

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 evaluated configuration instructions in the guidance documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

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

11 Security Target

The ST for this product's evaluation is Apple macOS 26 Tahoe: FileVault Security Target, Version 1.1, 2026-06-29 ([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]	PP-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
[ST]	Apple macOS 26 Tahoe: FileVault Security Target, Version 1.1, 2026-06-29
[CCGUIDE]	Apple macOS 26 Tahoe: FileVault Common Criteria Guide, Version 1.0, 2026-06-29
[ETR]	Evaluation Technical Report Apple macOS 26 Tahoe: FileVault, Version 1.1, 2026-07-28
[AAR]	Assurance Activity Report Apple macOS 26 Tahoe: FileVault, Version 1.1, 2026-07-28
[DTR]	Detailed Test Report Apple macOS 26 Tahoe: FileVault, Version 1.1, 2026-07-28