# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


# Validation Report for

# the

# Apple FileVault 2 on T2 systems running macOS Catalina 10.15

**Report Number:** CCEVS-VR-VID11078-2021

**Dated:** April 29, 2021

**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, PhD
Jerome Myers, PhD
DeRon Graves
*The Aerospace Corporation*

Clare Olin
*The MITRE Corporation*

## Common Criteria Testing Laboratory

Danielle Canoles
Rutwij Kulkarni
Dayanandini Pathmanathan

Acumen Security, LLC.


**Table of Contents**


**1 Executive Summary ..... 3**

**2 Identification ..... 4**

**3 Architectural Information ..... 5**

**4 Security Policy ..... 5**

**4.1 Logical Scope of the TOE ..... 5**

**4.2 Cryptographic Support (FCS) ..... 5**

**4.3 User Data Protection (FDP) ..... 6**

**4.4 Security Management (FMT) ..... 6**

**4.5 Protection of the TSF (FPT) ..... 6**

**5 Assumptions, Threats, and Clarification of Scope ..... 6**

**5.1 Assumptions ..... 6**

**5.2 Threats ..... 9**

**5.3 Clarification of Scope ..... 12**

**6 Documentation ..... 12**

**7 TOE Evaluated Configuration ..... 13**
**7.1 Evaluated Configuration ..... 13**
**8 IT Product Testing ..... 19**
**8.1 Developer Testing ..... 19**
**8.2 Evaluation Team Independent Testing ..... 20**
**9 Results of the Evaluation ..... 20**
**9.1 Evaluation of Security Target (ASE) ..... 20**
**9.2 Evaluation of Development Documentation (ADV) ..... 20**
**9.3 Evaluation of Guidance Documents (AGD) ..... 21**
**9.4 Evaluation of Life Cycle Support Activities (ALC) ..... 21**
**9.5 Evaluation of Test Documentation and the Test Activity (ATE) ..... 21**
**9.7 Vulnerability Assessment Activity (AVA) ..... 22**
**9.8 Summary of Evaluation Results ..... 23**
**10 Validator Comments and Recommendations ..... 24**
**11 Annexes ..... 25**
**12 Security Target ..... 26**
**13 Glossary ..... 27**
**14 Bibliography ..... 27**

# 1 Executive Summary

This Validation Report (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 for 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 tested and evaluated and any restrictions on the evaluated configuration. 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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Series Target of Evaluation (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 applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in April 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e]. This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against PP containing Assurance Activities, which are the interpretation of CEM work units specific to the technology described by the PP.

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 Compliance List.

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

- The Target of Evaluation [TOE]: the fully qualified identifier of the product as evaluated.
- The Security Target [ST], describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) 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 FileVault 2 on T2 systems running macOS Catalina 10.15 |
| **Protection Profile** | collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e]<br><br>collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e] |
| **Security Target** | Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Security Target, Version 2.5, April 19, 2021. |
| **Evaluation Technical Report** | Evaluation Technical Report for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 1.7, April 2021. |
| **CC Version** | Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Extended. |
| **Sponsor** | Apple Inc. |
| **Developer** | Apple Inc. |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>24 Research Blvd Suite 395<br>Rockville, MD 20850 |
| **CCEVS Validators** | Patrick Mallett, Jerome Myers, DeRon Graves, Clare Olin |

# 3 Architectural Information

The TOE is a full drive encryption product which supports authorization acquisition and encryption engine. The TOE is Unix-based operating system which leverages Apple T2 security processor to perform the full disk encryption. 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 TOE type is an authorization and encryption engine product. It satisfies all of the criterion to meet the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e].

# 4 Security Policy

## 4.1 Logical Scope of the TOE

The TOE implements the following security functional requirements from [FDE EE v2.0e] and [FDE AA v2.0e] as listed below:

## 4.2 Cryptographic Support (FCS)

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified (in **Table 4 CAVP Algorithm Testing References** of the ST).

### 4.3 User Data Protection (FDP)

The TOE encrypts all user data using XTS-AES 128 using a 256-bit key.

### 4.4 Security Management (FMT)

The TOE can perform management functions. The administrator has full access to carry out all management functions and the user have limited privilege. The Disk Utility program operating on macOS invokes management functionality of the AA component in the T2 chip.

### 4.5 Protection of the TSF (FPT)

The TOE implements the following protection of TSF data:

- Protection of Key and Key Material
- Power Saving States
- Timing of Power Saving States
- TSF Testing
- Trusted updates using digital signatures

The macOS (Operational Environment) retrieves the update package from the Apple update server and forwards the package to the AA component in the T2 chip. The TOE validates the digital signature for the package before it is installed.

## 5 Assumptions, Threats, and Clarification of Scope

### 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The following assumptions are drawn directly from the [FDE EE v2.0e] and [FDE AA v2.0e]:

| ID | Assumption |
|---|---|

| | |
|---|---|
| A.INITIAL_DRIVE_STATE | Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in “bad” sectors.<br>While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE preauthentication software) contain no protected data. |
| A.SECURE_STATE | Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization. |
| A.TRUSTED_CHANNEL | Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions. |
| A.TRAINED_USER/AA | Authorized users follow all provided user guidance, including keeping password/passphrases and external |

| **ID** | **Assumption** |
|---|---|
| | tokens securely stored separately from the storage device and/or platform. |

| | |
|---|---|
| A.TRAINED_USER/EE | Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system. |
| A.PLATFORM_STATE | The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product. |
| A.SINGLE_USE_ET | External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors. |
| A.POWER_DOWN | The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”. |
| A.PASSWORD_STRENGTH | Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected. |
| A.PLATFORM_I&A | The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface. |
| A.STRONG_CRYPTO | All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG. |

| | |
|---|---|
| A.PHYSICAL | The platform is assumed to be physically protected in its<br>Operational Environment and not subject to physical |
| **ID** | **Assumption** |
| | attacks that compromise the security and/or interfere with the platform's correct operation. |

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

The following threats are drawn directly from the [FDE EE v2.0e] and [FDE AA v2.0e]:

| ID | Threat |
|---|---|
| T.UNAUTHORIZED_DATA_ACCESS | The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks). |
| T.KEYING_MATERIAL_COMPROMISE/AA | Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of key material of equal importance to the data itself. Threat agents may look for key material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash. |

| | |
|---|---|
| T.KEYING_MATERIAL_COMPROMISE/EE | Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash, or TPMs. |

| **ID** | **Threat** |
|---|---|
| T.AUTHORIZATION_GUESSING/AA | Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release BEV or otherwise put it in a state in which it discloses protected data to unauthorized users. |
| T.AUTHORIZATION_GUESSING/EE | Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release DEKs or otherwise put it in a state in which it discloses protected data to unauthorized users. |
| T.KEYSPACE_EXHAUST | Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust the key space through brute force and give them unauthorized access to the data. |

| | |
|---|---|
| T.KNOWN_PLAINTEXT/EE | Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with known plaintext could allow an attacker to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device. |
| T.CHOSEN_PLAINTEXT/EE | Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device. |
| T.UNAUTHORIZED_UPDATE | Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen |
| **ID** | **Threat** |
| | update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software and/or firmware that bypasses the intended security features and provides them unauthorized access to data. |
| T.UNAUTHORIZED_FIRMWARE_MODIFY/EE | An attacker attempts to modify the firmware in the SED via a command from the AA or from the host platform that may compromise the security features of the TOE. |
| T.UNAUTHORIZED_FIRMWARE_MODIFY | An attacker attempts to replace the firmware on the SED via a command from the AA or from the host platform with a malicious firmware update that may compromise the security features of the TOE. |

### 5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e].
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 understanding of the TOE, technical sophistication, and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

# 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Apple Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Common Criteria Configuration Guide, Version 0.8, 19 April 2021 [AGD]

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE is comprised of the following software and hardware when configured in accordance with the documentation specified in Section 6. The TOE hardware consists of the Apple T2 Security Chip which is a custom silicon for the Mac. It 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 Password Acquisition component (AA) is the pre-boot component on the disk and captures the user password and passes it to the T2/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. The T2 chip is placed in the data path between the Intel chip and the storage, enabling it to encrypt/decrypt all data flowing between these two components.

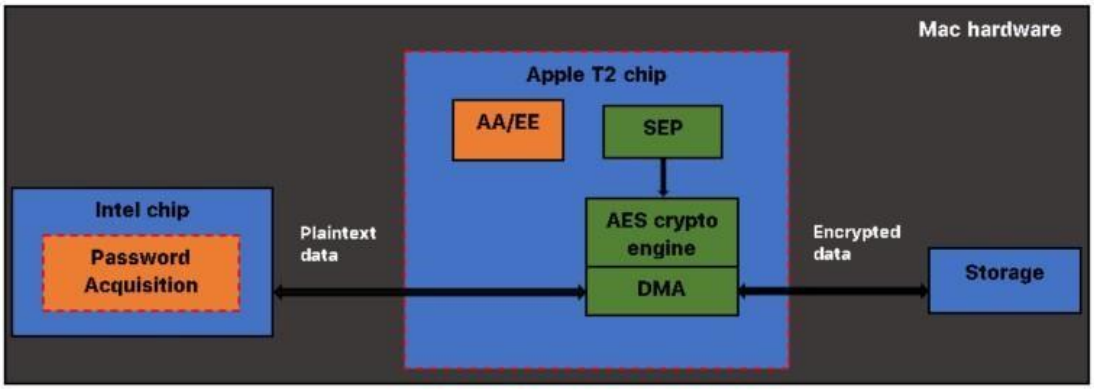


**Figure 1: Major components of TOE within red border**

The TOE also supports secure connectivity with an Apple update server as described in Table 2 below:

| Sr. No | Component | Required | Usage/Purpose Description for TOE performance |
|---|---|---|---|
| 1 | Apple update server | Yes | Provides the ability to download authentic signed updates. |

**Table 2: IT Environment Components** Table 3 below provides a list of supported platforms:

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2140B (Skylake) | |
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2150B (Skylake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2170B (Skylake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| iMac Pro<br><br>Model: A1862<br>Reference: iMac Pro1,1 | Late 2017 | Intel Xeon W-2191B (Skylake) | |
| Mac mini<br><br>Model: A1993<br>Reference: Macmini8,1 | 2018 | Intel Core i5-8500B (Coffee Lake) | |
| Mac mini<br><br>Model: A1993<br>Reference: Macmini8,1 | 2018 | Intel Core i7-8700B (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i5-8279U (Coffee Lake) | |
| MacBook Pro<br><br>Model: 1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i5-8259U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | Mid 2018 | Intel Core i7-8750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | Mid 2018 | Intel Core i7-8559U (Coffee Lake) | |

| | | | |
|---|---|---|---|
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | Mid 2018 | Intel Core i7-8850H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | Mid 2018 | Intel Core i9-8950HK (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | Mid 2018 | Intel Core i9-8950HK (Coffee Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| MacBook Air<br><br>Model: A1932<br>Reference: MacBookAir8,1 | Late 2018 | Intel Core i5-8210Y (Amber Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| MacBook Air<br><br>Model: A1932<br>Reference: MacBookAir8,2 | 2019 | Intel Core i5-8210Y (Amber Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3223 (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3235 (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3245 (Cascade Lake) | |
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3265M (Cascade Lake) | |

| | | | |
|---|---|---|---|
| Mac Pro<br><br>Model: A1991<br>Reference: Mac Pro7,1 | 2019 | Intel Xeon W-3275M (Amber Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | 2019 | Intel Core i5-8279U (Amber Lake) | |
| MacBook Pro<br><br>Model: A2159<br>Reference: MacBookPro15,4 | 2019 | Intel Core i5-8257U (Amber Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core i7-9750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1989<br>Reference: MacBookPro15,2 | 2019 | Intel Core i7-8569U (Coffee Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| MacBook Pro<br><br>Model: A2159<br>Reference: MacBookPro15,4 | 2019 | Intel Core i7-8557U (Coffee Lake) | Apple T2 (ARM64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| MacBook Pro:<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i7-9750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core i9-9880H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,1 | 2019 | Intel Core i9-9980HK (Coffee Lake) | |

| | | | |
|---|---|---|---|
| MacBook Pro<br><br>Model: A1990<br>Reference: MacBookPro15,3 | 2019 | Intel Core i9-9880H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i9-9880H (Coffee Lake) | Apple T2(ARM 64)<br><br>Processor T2 (processor family |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBookPro16,1 | 2019 | Intel Core i9-9980HK (Coffee Lake) | arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i7-9750H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i9-9880H (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2141<br>Reference: MacBook Pro16,4 | 2019 | Intel Core i9-9980HK (Coffee Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2019 | Intel Core i5-10500 (Ice Lake) | |

| Device | Year | Intel Processor | Apple T2 Chip |
|---|---|---|---|
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3275M (Cascade Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3265M (Cascade Lake) | |

| | | | |
|---|---|---|---|
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3245 (Cascade Lake) | |
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3235 (Cascade Lake) | |

| | | | |
|---|---|---|---|
| Mac Pro (rack)<br><br>Model: A2304<br>Reference: MacPro7,1 | 2019 | Intel Xeon W-3223 (Cascade Lake) | Apple T2(ARM 64)<br><br>Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15 |
| MacBook Air<br><br>Model: A2179<br>Reference: MacBook Air9,1 | 2020 | Intel Core i5-1030NG7 (Ice Lake) | |
| MacBook Air<br><br>Model: A2179<br>Reference: MacBook Air9,1 | 2020 | Intel Core i7-1060NG7 (Ice Lake) | |
| MacBook Pro<br><br>Model: A2289<br>Reference: MacBook Pro16,3 | 2020 | Intel Core i5-8257U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2289<br>Reference: MacBook Pro16,3 | 2020 | Intel Core i7-8557U (Coffee Lake) | |
| MacBook Pro<br><br>Model: A2251<br>Reference: MacBook Pro16,2 | 2020 | Intel Core i5-1037NG7 (Ice Lake) | |
| MacBook Pro<br><br>Model: A2251<br>Reference: MacBook Pro16,2 | 2020 | Intel Core i7-1068NG7 (Ice Lake) | |
| Device | Year | Intel Processor | Apple T2 Chip |

| | | | |
|---|---|---|---|
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i5-10600 (Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i7-10700K (Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,1 | 2020 | Intel Core i9-10910 (Coffee Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,2 | 2020 | Intel Core i7-10700K (Ice Lake) | |
| iMac<br><br>Model: A2115<br>Reference: iMac20,2 | 2020 | Intel Core i9-10910 (Coffee Lake) | |

**Table 3: Platform specifications**

Note: The Apple T2 Security Chip is the same exact chip across all platforms. All processing for Cryptography related to FileVault (FDE) is all performed using the Apple T2 / SEP rather than the Intel chipset, so multiple Intel Chips or microarchitectures play no role in the processing (encryption/decryption) and the management of those keys for data under FileVault.

# 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

## 8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

### 8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. A description of the tests tools and the test configuration may be found in Section 4 of the AAR.

# 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Apple FileVault 2 on T2 systems running macOS Catalina 10.15 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the FDE EE v2.0e and FDE AA v2.0e.

## 9.1 Evaluation of Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Apple FileVault 2 on T2 systems running macOS Catalina 10.15 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e].

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

## 9.2 Evaluation of Development Documentation (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

## 9.3 Evaluation of Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was adequately identified.

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

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

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e] and that the conclusion reached by the evaluation team was justified.

## 9.7 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities on 04/20/2021 and did not discover any issues with the TOE.

The table below presents items that were searched by CPE:

| Component | CPE |
|---|---|
| Apple Mac Mini i5 8500B | cpe:2.3:h:apple:Mac:mini:*:*:*:*:macOS:i5-8500B:Macmini |
| Apple MacBook Air i7 1060NG-7 | cpe:2.3:h:apple:MacBook:Air:*:*:*:*:macOS:i7-1060NG-7:MacBookAir |
| Apple MacBookPro i7-8557U | cpe:2.3:h:apple:MacBook:Pro:*:*:*:*:macOS:i7-8557U:MacBookPro |
| Apple sepOS 10.15.7 | cpe:2.3:o:apple:sepOS:10.15.7:*:*:*:*:TxFW:Apple_T_Series:TxFW_4.7 |
| Apple sepOS 10.15.6 | cpe:2.3:o:apple:sepOS:10.15.6:*:*:*:*:TxFW:Apple_T_Series:TxFW_4.6 |
| Apple T2 Security Chip | cpe:2.3:h:apple:Apple_Tx_Security_Chip:T2:*:*:*:*:TxFW:Apple_T2:iBridge |
| Apple corecrypto kernel | cpe:2.3:*:apple:CoreCrypto_Kernel:10:10.15.7:*:*:*:macOS:x86_64:* |
| Apple Secure Key Store sepOS | cpe:2.3:*:apple:Secure_Key_Store:10:10.15:*:*:TxFW:sepOS:Apple_T_Series:* |

Three public sources were searched for publicly reported vulnerabilities. The sources are provided below:

- cve.mitre.org,
- National Vulnerability Database (nvd.nist.gov) and
- kb.cert.org

The terms below were searched:

- FileVault,
- sepOS,
- corecrypto
- drive encryption,
- disk encryption,
- key destruction/sanitization,
- key caching and
- password caching
- Apple FileVault 2
- Apple FileVault 2 on T2 systems running macOS Catalina 10.15

The TOE is the “Apple FileVault 2 on T2 systems running macOS 10.15 Catalina”. All platform libraries and frameworks are distributed together, and vulnerabilities are reported under the platform OS CPE. The evaluated TOE version is macOS 10.15.7 Catalina.

The CCTL conducted the testing on Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7.

**Apple T2 Security Chip and remote testing rationale is provided below:**

For the following eight (8) SFRs, the vendor conducted the testing on an Intel Core i7 Coffee Lake 8557U (Note: This model includes the Apple T2 Security Chip and this chip is same across all Mac devices) and the same exact test evidence was reused across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. The motivation to reuse the same evidence from Intel Core i7 Coffee Lake 8557U across the two (2) TOE models is because the TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave. Because encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel microarchitectures are irrelevant to the protection of Data at Rest using FileVault. This rationale was accepted by NIAP Validators during the synch meeting on 02/19/2021.

The testing for the following eight (8) SFRs was conducted by the vendor personnel, and the CCTL remotely witnessed this testing. The CCTL submitted the remote testing request to NIAP on 02/04/2021 and NIAP approved the request on 03/03/2021.

1. FCS_CKM.4(b) Test#1 [EE] 2. FCS_CKM.4(b) Test#2 [EE]
3. FCS_CKM.4(b) Test#3 [EE]
4. FCS_CKM.4(d) Test#1 [AA+EE] 5. FCS_CKM.4(d) Test#2 [AA+EE]
6. FCS_CKM.4(d) Test#3 [AA+EE]
7. FCS_VAL_EXT.1 and
8. FPT_PWR_EXT.1

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e]., and that the conclusion reached by the evaluation team was justified.

## 9.8 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e] and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version

2.0 + Errata 20190201 [FDE AA v2.0e]., and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments and Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Common Criteria Configuration Guide, Version 0.8, 19 April 2021 document. 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, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Security Target, Version 2.5, 19 April 2021 [ST]

# 13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **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.

# 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:


1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, Version 3.1 Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
5. collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201 [FDE EE v2.0e]. PP Date: 01 February 2019.
6. collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201 [FDE AA v2.0e]. PP Date: 01 February 2019.

7. Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Security Target, Version 2.5, 19 April 2021 [ST].

8. Apple Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Common Criteria Configuration Guide, Version 0.8, 19 April 2021 [AGD].

9. Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Key Management Description, Version 2.2, 19 March 2021 [KMD].

10. Assurance Activity Report for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 1.9, 30 April 2021 [AAR].

11. Evaluation Technical Report for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 1.8, 29 April 2021 [ETR].

12. Vulnerability Assessment for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 0.7, 20 April 2021 [AVA].

13. Test Report of Intel Core i5-8500B (Coffee Lake i5) for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 2.2, 30 April 2021 [ATE].

14. Test Report of Intel Core i7-1060NG7 (Ice Lake i7) for Apple FileVault 2 on T2 systems running macOS Catalina 10.15, Version 2.2, 30 April 2021 [ATE].