National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report for macOS Catalina 10.15

Report Number:	**CCEVS-VR-11077-2020**
Dated:	**September 23, 2020**
Version:	**1.2**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Chris Thorpe
Clare Olin
Randy Heimann
Linda Morrison

Common Criteria Testing Laboratory

Dayanandini Pathmanathan
Rutwij Kulkarni
Yogesh Pawar
Varsha Shetye

Table of Contents

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 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 September 2020. 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 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOS PP v4.2.1]. 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 Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). 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	macOS Catalina 10.15
Protection Profile	Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOS PP v4.2.1]
Security Target	macOS Catalina 10.15 Security Target, Version 2.0, 18 September 2020
Evaluation Technical Report	Evaluation Technical Report for macOS Catalina 10.15, Version 1.7, 18 September 2020
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 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Paul Bicknell Chris Thorpe Clare Olin

	Randy Heimann Linda Morrison

3 Architectural Information

- TOE is a general-purpose operating system (GPOS) which runs on Mac mini, MacBook Air, MacBook Pro and Mac Pro iPad which include the T2 chip. The macOS Catalina is a Unix-based graphical operating system. The macOS core is a POSIX compliant operating system built on top of the XNU kernel with standard Unix facilities available from the command line interface.
- The TOE type is a general-purpose operating system. It satisfies all of the criterion to meet the Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOS PP v4.2.1].

4 Security Policy

Logical Scope of the TOE

The TOE implements the following security functional requirements from [GPOSPP] as listed below:

4.1 Audit Data Generation (FAU)

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in GPOS PP. Audit events are generated for the following audit functions:

- Start-up and shut-down of the audit functions;
- Authentication events (Success/Failure);
- Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)
- Privilege or role escalation events (Success/Failure)

Each audit record contains the date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event.

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 below:

Algorithm	Standard	CAVP Certificates
AES	• AES-CBC (as defined in NIST SP 800-38A)	**CoreCrypto User Certs:** A7 (c_asm), A8 (c_ltc), A11 (c_glad), A19 (asm_aesni), A21 (c_aesni), A25 (asm_x86) **CoreCrypto Kernel Certs:** A15 (c_asm), A20 (asm_aesni), A23 (c_aesni), A24 (asm_x86), A25 (asm_x86)
	• AES-GCM (as defined in NIST SP 800-38D)	**CoreCrypto User Certs:** A7 (c_asm), A8 (c_ltc), A10 (vng_asm), A21 (c_aesni), A31 (vng_aesni) **CoreCrypto Kernel Certs:** A13 (vng_asm), A28 (vng_aesni)
RSA	• FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3.	**CoreCrypto User Certs:** A8 (c_ltc), A22 (c_avx), A27 (c_sse3), A33 (c_avx2) **CoreCrypto Kernel Certs:** A26 (c_avx2), A30 (c_avx), A34 (c_sse3)
ECDSA	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	**CoreCrypto User Certs:** A8 (c_ltc), A22 (c_avx), A27 (c_sse3),

Algorithm	**Standard**	**CAVP Certificates**
		A33 (c_avx2) **CoreCrypto Kernel Certs:** A26 (c_avx2), A30 (c_avx), A34 (c_sse3)
KAS/CVL ECC	- NIST Special Publication 800-56A	**CoreCrypto User Certs:** A8 (c_ltc)
HMAC	- Keyed-hash message authentication services in conforming to FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard	**CoreCrypto User Certs:** A8 (c_ltc), A22 (c_avx), A27 (c_sse3), A29 (vng_intel), A33 (c_avx2) **CoreCrypto Kernel Certs:** A26 (c_avx2), A30 (c_avx), A32 (vng_intel), A34 (c_sse3)
SHS	- NIST FIPS Pub 180-4.	**CoreCrypto User Certs:** A8 (c_ltc), A22 (c_avx) , A27 (c_sse3), A29 (vng_intel), A33 (c_avx2) **CoreCrypto Kernel Certs**: A26 (c_avx2), A30 (c_avx), A32 (vng_intel), A34 (c_sse3)
DRBG	- CTR_DRBG (AES)	**CoreCrypto User Certs:** A7 (c_asm) A8 (c_ltc), A10 (vng_asm), A21 (c_aesni), A31 (vng_aesni) **CoreCrypto Kernel Certs:** A15(c_asm), A23 (c_aesni), A13 (vng_asm), A28 (vng_aesni)

Algorithm	Standard	CAVP Certificates
CVL TLS v1.2	• KDF 800-108	**CoreCrypto User Certs:** A8 (c_ltc), A22 (c_avx), A27 (c_sse3) **CoreCrypto Kernel Certs:** A34 (c_sse3)

Table 2 CAVP Algorithm Testing References

4.3 User Data Protection (FDP)

The TOE implements access controls which prevents unprivileged users from accessing files and directories owned by other users. The TOE provides an interface which allows VPN client to protect all IP traffic.

4.4 Identification and Authentication (FIA)

All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication, authentication based on username and a PIN that releases asymmetric key stored in OE-protected storage and X509 certificate-based authentication. The TOE will lock out user accounts after a defined number of unsuccessful authentication attempts have been met.

4.5 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.

4.6 Protection of the TSF (FPT)

The TOE implements the following protection of TSF data:

- Access Controls
- Randomize process address space memory locations with 16 bit of entropy.
- Stack buffer overflow protection is used
- Verification of integrity of the boot-chain and operating system executable code and application executable code.
- Trusted software updates using digital signatures.

4.7 Trusted Path/Channels (FTP)

The TOE supports TLS v1.2 for trusted channel and trusted path communications.

4.8 TOE Access (FTA)

Before establishing a user session, the TOE will display an advisory warning message regarding unauthorized use of the OS.

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 [GPOSPP]:

ID	Assumption
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

Table 3 Assumptions

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 [GPOSPP]:

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.

ID	Threat
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

Table 4 Threats

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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOS PP v4.2.1].
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- 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 of 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 macOS Catalina 10.15 Common Criteria Configuration Guide, Version 1.7 dated 18 September 2020

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE includes the operating system macOS Catalina 10.15 (Build 19G73) and the security processor (T2) (SEPOS build 17P5300).

The Apple T2 Security Chip is custom silicon for the Mac. It contains the Secure Enclave processor which provides security related functionality that secures Touch ID data and provides the foundation for new encrypted storage and secure boot capabilities. Each of the TOE platforms includes both the Apple T2 Security Chip (T2) and an Intel CPU where the TOE runs. *NOTE: The TOE boundary would include the T2 chip and the Intel CPU.*
The TOE will comply with [Use Case 1] End User Devices as outlined in Section 1.4 of the GPOS PP.

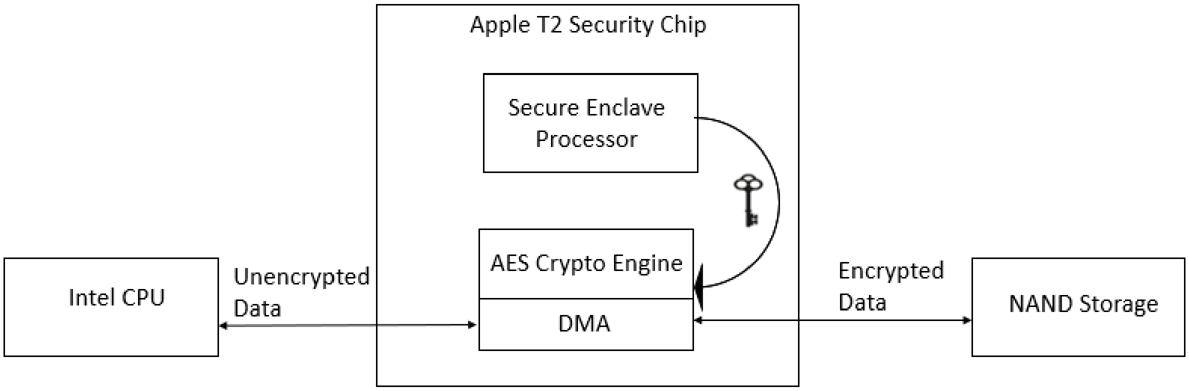

Figure 1: Apple T2 Security Chip and SEP

Devices covered by this Evaluation

Micro-architecture	Processor - Intel Core	Device Family	Hardware Reference	Model	Marketing Release Name
Amber Lake	Intel i5-8210Y	MacBook Air	MacBookAir 8,2	A1932	2019
Amber Lake	Intel i5-8210Y	MacBook Air	MacBookAir 8,1	A1932	Late 2018
Coffee Lake	Intel i5-8257U	MacBook Pro	MacBook Pro16,3	A2289	2020, 13-inch
Coffee Lake	Intel i5-8257U	MacBook Pro	MacBookPro15,4	A2159	2019 13-inch (Touch Bar, 2TB 3)

Coffee Lake	Intel i5-8259U	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)
Coffee Lake	Intel i5-8279U	MacBook Pro	MacBookPro15,2	A1989	2019, 13-inch (Touch Bar)
Coffee Lake	Intel i5-8279U	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)
Coffee Lake	Intel i5-8500B	Mac mini	Macmini8,1	A1993	2018
Coffee Lake	Intel i7-8557U	MacBook Pro	MacBook Pro16,3	A2289	2020, 13-inch
Coffee Lake	Intel i7-8557U	MacBook Pro	MacBookPro15,4	A2159	2019 13-inch (Touch Bar, 2TB 3)
Coffee Lake	Intel i7-8559U	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)
Coffee Lake	Intel i7-8569U	MacBook Pro	MacBookPro15,2	A1989	2019, 13-inch (Touch Bar)
Coffee Lake	Intel i7-8700B	Mac mini	Macmini8,1	A1993	2018
Coffee Lake	Intel i7-8750H	MacBook Pro	MacBookPro15,1	A1990	Mid 2018, 15-inch (Touch Bar)
Coffee Lake	Intel i7-8850H	MacBook Pro	MacBookPro15,3	A1990	Mid 2018, 15-inch (Touch Bar)

Coffee Lake	Intel i7-9750H	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)
Coffee Lake	Intel i7-9750H	MacBook Pro	MacBookPro16,1	A2141	2019, 16-inch
Coffee Lake	Intel i9-8950HK	MacBook Pro	MacBookPro15,1	A1990	Mid 2018, 15-inch (Touch Bar)
Coffee Lake	Intel i9-8950HK	MacBook Pro	MacBookPro15,3	A1990	Mid 2018, 15-inch (Touch Bar)
Coffee Lake	Intel i9-9880H	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)
Coffee Lake	Intel i9-9880H	MacBook Pro	MacBookPro15,3	A1990	2019, 15-inch (Touch Bar)
Coffee Lake	Intel i9-9880H	MacBook Pro	MacBookPro16,1	A2141	2019, 16-inch
Coffee Lake	Intel i9-9980HK	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)
Coffee Lake	Intel i9-9980HK	MacBook Pro	MacBookPro15,3	A1990	2019, 15-inch (Touch Bar)
Coffee Lake	Intel i9-9980HK	MacBook Pro	MacBookPro16,2	A2141	2019, 16-inch
Ice lake	Intel i5-1030NG7	MacBook Air	MacBookAir9,1	A2179	2020
Ice Lake	Intel i5-1038NG7	MacBook Pro	MacBook Pro16,2	A2251	2020, 13-inch
Ice Lake	Intel i7-1060NG7	MacBook Air	MacBookAir9,1	A2179	2020
Ice Lake	Intel i7-1068NG7	MacBook Pro	MacBook Pro16,2	A2251	2020, 13-inch

Skylake	Intel Xeon W-2140B	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017
Skylake	Intel Xeon W-2150B	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017
Skylake	Intel Xeon W-2170B	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017
Skylake	Intel Xeon W-2191B	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017
Cascade Lake	Intel Xeon W-3223	Mac Pro	MacPro7,1	A1991	2019
Cascade Lake	Intel Xeon W-3223	Mac Pro(rack)	MacPro7,1	A2304	2019
Cascade Lake	Intel Xeon W-3235	Mac Pro	MacPro7,1	A1991	2019
Cascade Lake	Intel Xeon W-3235	Mac Pro(rack)	MacPro7,1	A2304	2019
Cascade Lake	Intel Xeon W-3245	Mac Pro	MacPro7,1	A1991	2019
Cascade Lake	Intel Xeon W-3245	Mac Pro(rack)	MacPro7,1	A2304	2019
Cascade Lake	Intel Xeon W-3265M	Mac Pro	MacPro7,1	A1991	2019
Cascade Lake	Intel Xeon W-3265M	Mac Pro(rack)	MacPro7,1	A2304	2019
Cascade Lake	Intel Xeon W-3275M	Mac Pro	MacPro7,1	A1991	2019
Cascade Lake	Intel Xeon W-3275M	Mac Pro(rack)	MacPro7,1	A2304	2019

Table 5 Platform specifications

7.2 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

Functions	Exclusion discussion
Two-Factor Authentication	Two-factor authentication is an extra layer of security for an Apple ID used in the Apple store, iCloud and other Apple services. It is designed to enhance the security on these on-line Apple accounts. This feature is outside the scope of the evaluation.
Bonjour	Bonjour is Apple's standards-based, zero configuration network protocol that lets devices find services on a network. This feature is outside the scope of the evaluation.
VPN Split Tunnel	VPN split tunnel is not included in the evaluation and must be disabled in the mobile device configurations meeting the requirements of this CC evaluation.
Siri Interface	The Siri interface supports some commands related to configuration settings. This feature is not included in the evaluation and must be disabled in the mobile device configurations that meet the requirements of this CC evaluation.

Table 6 Excluded Functionality

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 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [OS PP v4.2.1]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

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 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 GPOS PP v4.2.1.

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 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [OS PP v4.2.1].

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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1]. 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1]. 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1]. 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1] 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 11 June 2020 , 18 August 2020 and 16 September 2020 and did not discover any issues with the TOE. The terms used for the search were as follows:

- Apple macOS 10.15.6
- Apple macOS 10.15.5
- Apple macOS 10.15.4
- Apple sepOS 10.15.4
- Apple sepOS 10.15.3
- TLS 1.2

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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1]., 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 Protection Profile for General Purpose Operating Systems Version 4.2.1 [GPOS PP v4.2.1]., and correctly verified that the product meets the claims in the ST.

10 Validator Comments and Recommendations

The validation team recommends that the consumer pay particular attention to the installation guidance to ensure the product is placed into the evaluated configuration. The functionality that was evaluated was scoped exclusively to the security functional requirements specified in the Security Target.

macOS Catalina provides capabilities that are in addition to those evaluated. Only the functionality implemented by the SFR's within the Security Target was evaluated.
Note that the evaluated version of the product includes macOS Catalina 10.15.6. The product, when shipped, may not have the exact version that was tested, and if it does not, then the administrator should upgrade to the CC evaluated version.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The excluded functionality is specified in section 7.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

ST Reference: macOS Catalina Security Target v2.0, dated September 18, 2020

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. Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22 April 2019.
6. macOS Catalina 10.15 Security Target, Version 2.0, 18 September 2020 [ST]
7. Apple macOS Catalina 10.15 Common Criteria Configuration Guide, Version 1.7, 18 September 2020 [AGD]
8. Assurance Activity Report for macOS Catalina 10.15, Version 1.8, 18 September 2020 [AAR]
9. Vulnerability Assessment for macOS Catalina 10.15, Version 1.3, 16 September 2020 [AVA]
10. Evaluation Technical Report for macOS Catalina 10.15, Version 1.7, 18 September 2020 [ETR]
11. Test Report of Intel Core i5-8500B (Coffee Lake i5) for macOS Catalina 10.15, Version 1.7, 17 September 2020
12. Test Report of Intel Core i7-1060NG7 (Ice Lake i7) for macOS Catalina 10.15, Version 1.2, 16 September 2020