intertek
acumen
security

Assurance Activity Report for macOS Catalina 10.15

macOS Catalina 10.15 Security Target
Version 2.0

Protection Profile for General Purpose Operating Systems, Version 4.2.1

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Apple, Inc.

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Apple, Inc.

Evaluation Personnel:
Dayanandini Pathmanathan
Rutwij Kulkarni
Yogesh Pawar
Varsha Shetye

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History:

Version	Date	Changes
1.0	21-04-2020	Initial Draft
1.1	19-08-2020	Updated ST and AGD
1.2	20-08-2020	Internal review
1.3	24-08-2020	Updated ST
1.4	27-08-2020	Updated ST and AGD
1.5	28-08-2020	Internal review
1.6	16-9-2020	Addressing validator comments
1.7	17-9-2020	Final version
1.8	18-9-2020	Updated final versions of documents

Table of Contents

1 TOE Overview

The 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. 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.

2 TOE Description

The TOE includes the operating system macOS Catalina 10.15.6 (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 coprocessor 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

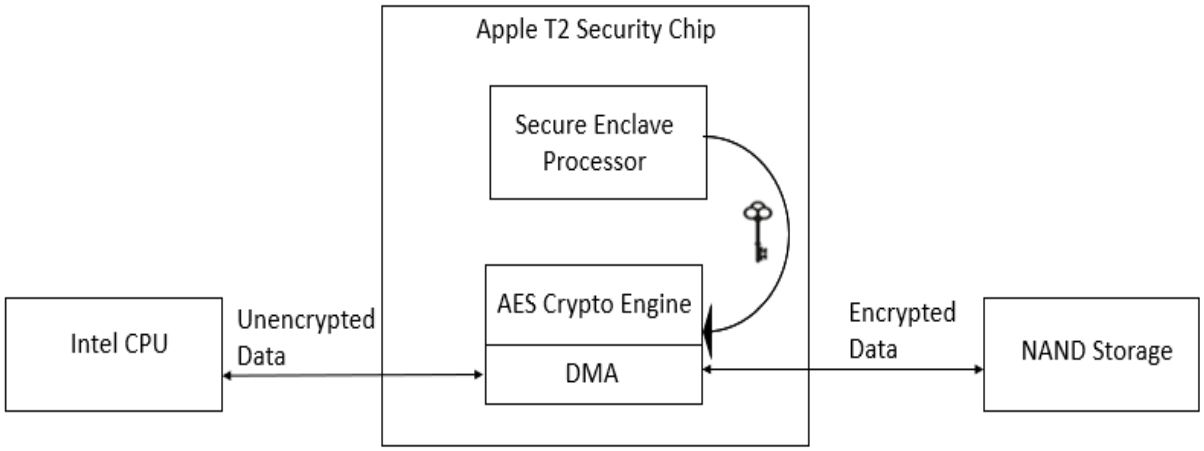

Figure 1: Apple T2 Security Chip and SEP

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	MacBookAir8,2	A1932	2019
Amber Lake	Intel i5-8210Y	MacBook Air	MacBookAir8,1	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 1: Platform specifications

3 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within GPOSPP v4.2.1 based upon the core SFRs and those implemented based on selections within the PP.

The following table identifies each of the Assurance Activities (testing and documentation review) executed for this evaluation.

Requirements	Descriptions
FAU_GEN.1	Audit Data Generation (Refined)
FCS_CKM.1	Cryptographic Key Generation (Refined)
FCS_CKM.2	Cryptographic Key Establishment (Refined)
FCS_CKM_EXT.4	Cryptographic Key Destruction
FCS_COP.1(1)	Cryptographic Operation - Encryption/Decryption (Refined)
FCS_COP.1(2)	Cryptographic Operation - Hashing (Refined)
FCS_COP.1(3)	Cryptographic Operation - Signing (Refined)
FCS_COP.1(4)	Cryptographic Operation - Keyed-Hash Message Authentication (Refined)
FCS_RBG_EXT.1	Random Bit Generation
FCS_STO_EXT.1	Storage of Sensitive Data
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Protocol
FCS_TLSC_EXT.4	TLS Client Protocol

FDP_ACF_EXT.1	Access Controls for Protecting User Data
FIA_AFL.1	Authentication Failure Management (Refined)
FIA_UAU.5	Multiple Authentication Mechanisms (Refined)
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_MOF_EXT.1	Management of security functions behavior
FMT_SMF_EXT.1	Specification of Management Functions
FPT_ACF_EXT.1	Access controls
FPT_ASLR_EXT.1	Address Space Layout Randomization
FPT_SBOP_EXT.1	Stack Buffer Overflow Protection
FPT_TST_EXT.1	Boot Integrity
FPT_TUD_EXT.1	Trusted Update
FPT_TUD_EXT.2	Trusted Update for Application Software
FTP_ITC_EXT.1	Trusted channel communication
FTP_TRP.1	Trusted Path
FTA_TAB.1	Default TOE access banners

Table 2: SFRs

4 Test Equivalency Justification

4.1 Introduction

This document provides a testing equivalency analysis for the macOS Catalina 10.15.6. This analysis provides an explanation of the differences between each of the models included within the TOE boundary and provides an analysis of the impact each of the differences have on the TSF functionality.

4.2 Architectural Description

The TOE is a general-purpose operating system (GPOS) which runs on Apple Mac computers with the T2 chip which includes Mac Pro, iMac Pro, Mac mini, MacBook Pro, and MacBook Air. The macOS Catalina is a Unix-based graphical operating system. The macOS core is a Mach/BSD hybrid XNU kernel with standard Unix and POSIX compliant facilities available from the command line interface.

4.3 Analysis

The following table compares the Operating System, Micro-architecture, Generation, Processor, Instruction Set, Device Family, Hardware Reference, Model and Marketing Release Name, that runs on each of the included TOE platforms. All Systems map to the same set of CAVP certificates as indicated below.

Micro-architecture	Processor - Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name
Amber Lake	Intel i5-8210Y	**Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2**	**MacBook Air**	MacBookAir8,2	A1932	2019
Amber Lake	Intel i5-8210Y		**MacBook Air**	MacBookAir8,1	A1932	Late 2018
Coffee Lake	Intel i5-8257U		**MacBook Pro**	MacBookPro15,4	A2159	2019 13-inch (Touch Bar, 2TB 3)
Coffee Lake	Intel I5-8257U		**MacBook Pro**	MacBook Pro16,3	A2289	2020, 13-inch
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**	MacBook Pro15,1	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**	MacBookPro16,1	A2141	2019, 16-inch

Ice lake	Intel i5-1030NG7	**AVX-512 Not Used by CoreCrypto**	**MacBook Air**	MacBookAir9,1	A2179	2020, 13-inch scissor
Ice Lake	Intel i5-1038NG7		**MacBook Pro**	MacBook Pro16,2	A2251	2020, 13-inch
Ice Lake	Intel i7-1068NG7		**MacBook Pro**	MacBook Pro16,2	A2251	2020, 13-inch
Ice Lake	Intel i7-1060NG7		**MacBook Air**	MacBookAir9,1	A2179	2020, 13-inch scissor
Skylake	Intel Xeon W-2140B	**AVX-512 Not Used by CoreCrypto**	**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 3: Device Microarchitecture

The TOE is Apple macOS Catalina 10.15.6. The test subset was determined by the following factors:

1. Model A1932 uses Amber Lake, models A1989, A2159, A1993, A2141 and A1990 use Coffee Lake, and models A1862 and A1991 use Skylake processors.
2. All the above processors share the same Broadwell 14-nm process and Skylake microarchitecture. The differences between Skylake, Amber Lake, Coffee Lake and Cascade Lake are only based on optimization and performance. There is no architectural difference between both. Also, there are no differences between them based on their security features.
3. The A1862 model uses Skylake Xeon W processors and the A1991 /A2304 models use Cascade Lake processor. The Cascade Lake processor is also based on the Skylake microarchitecture and like Skylake, also uses a 14 nm fabrication process. The Cascade Lake also has the DL boost in addition to Skylake microarchitecture. The differences between Skylake and Cascade Lake are only based on optimization and performance. There is no architectural difference between both. The Skylake, Cascade Lake, Coffee Lake and Amber Lake are all similar in the security features they support.
4. The Ice Lake processor family is the next generation Intel Core processor family. These processors utilize Intel's industry-leading 10 nm+ fabrication process. 10nm+ features higher performance through higher drive current for the same power envelope. The key changes from Skylake are as follows:
    a. Enhanced 10nm+

b. Sunny Cove (A high performance 10nm x86 core microarchitecture designed by Intel)
c. Introduced several new instructions:
    i. SHA - Hardware acceleration for SHA hashing operations
    ii. CLWB - Force cache line write-back without flush
    iii. RDPID - Read Processor ID
    iv. AVX-512 (originally introduced in Skylake (Server) but only now in client)
    v. AVX512F - AVX-512 Foundation
    vi. AVX512CD - AVX-512 Conflict Detection
    vii. AVX512BW - AVX-512 Byte and Word
    viii. AVX512DQ - AVX-512 Doubleword and Quadword
    ix. AVX512VL - AVX-512 Vector Length
d. Additional AVX-512 extensions:
    i. AVX512VPOPCNTDQ - AVX-512 Vector Population Count Doubleword and Quadword
    ii. AVX512VNNI - AVX-512 Vector Neural Network Instructions
    iii. AVX512GFNI - AVX-512 Galois Field New Instructions
    iv. AVX512VAES - AVX-512 Vector AES
    v. AVX512VBMI2 - AVX-512 Vector Bit Manipulation, Version 2
    vi. AVX512BITALG - AVX-512 Bit Algorithms
    vii. AVX512VPCLMULQDQ - AVX-512 Vector Vector Carry-less Multiply
e. SSE_GFNI - SSE-based Galois Field New Instructions
f. AVX_GFNI - AVX-based Galois Field New Instructions
g. Split Lock Detection - detection and cause an exception for split locks
h. Fast Short REP MOV

5. The OS is identical on each of the platforms, and there are no differences in the crypto libraries on the platform themselves.

Based on the above factors, Acumen Security tested one CPU model of Coffee Lake microprocessor architecture and one CPU model of Ice Lake microprocessor architecture.

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the GPOS PP.

4.4 Platform/Hardware Differences

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF functionality. For the hardware appliances, the hardware within the

TOE only differs by configuration and performance. There are no hardware specific dependencies of the product.

4.5 Software/OS Dependencies

The underlying OS is installed with the application level software on each of the platforms. The underlying OS for all models within the TOE is macOS Catalina 10.15.6.

4.6 Differences in TOE Software Binaries

All software binaries compiled in the TOE software are identical including the version of the crypto library. There are no differences between the included libraries. Because the OS is identical on each of the tested platforms, there are no differences in the crypto libraries on the platform themselves.

4.7 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical including the version of the library regardless of the platform for which the software is compiled. There are no differences between the included libraries. Because the OS is identical on each of the tested platforms, there are no differences in the libraries on the platforms themselves.

4.8 TOE Functional Differences

The TOE boundary on each hardware model provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available for each of these devices. Each device runs the same version of software.

4.9 Test Subset Justification/Rationale

Based on the analysis above, it is recommended that the TOE be tested on a platform running, Intel Core i5-8500B (Coffee Lake i5) and Intel Core i7-1060NG7 (Ice Lake i7).

The following platforms will be used for testing:

Models	Processors	Operating System
A1993	Intel Core i5-8500B (Coffee Lake i5)	macOS Catalina 10.15.6
A2179	Intel Core i7-1060NG7 (Ice Lake i7)	macOS Catalina 10.15.6

Table 5: Testing Platforms

5 Test Diagram

5.1 Testbed Diagram – Audit/Auth/TLSS/X.509/Update

Below is a visual representation of the components included in the test bed:

The following provides configuration information about each device on the test network.

5.1.1 Test Bed for Intel Core i5-8500B (Coffee Lake i5):

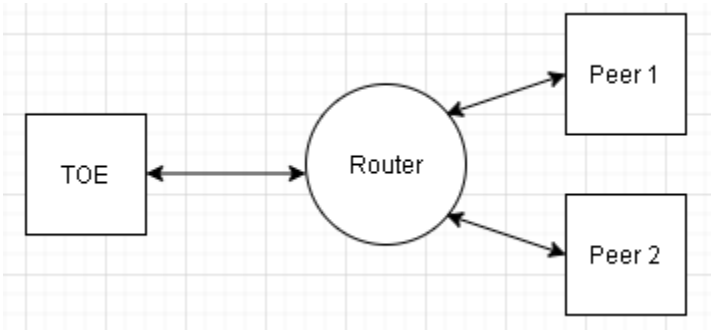

Figure 2: Test Bed #1 for Coffeelake i5

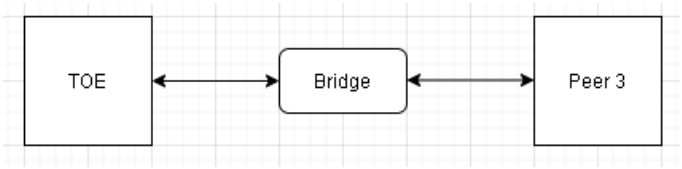

Figure 3: Test Bed #2 for CoffeeLake i5

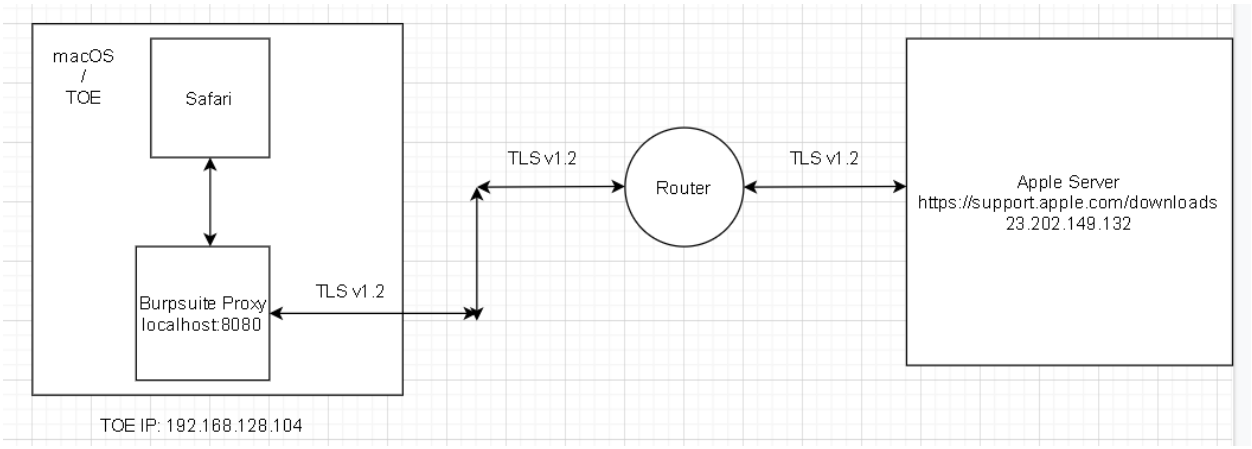

Figure 4: Test Bed for #3 CoffeeLake i5 FPT_TUD_Ext.1.1 and FPT_TUD_Ext.2.1

Sr. No	Name	OS	Credentials	Version	Function	Protocols	IP address	MAC Address	Tools (version)	Time
1	Apple Mac Mini Intel Core	Apple macOS Catalina	acumensec /acumense c	10.15.6	TOE	TLS 1.2/HTTP S	192.168.1 28.104 10.1.9.15	f0:18:98 :f0:cb:a4	Safari 13.0.5 Proxy-BurpSuit e Pro v2020.2	Manually set and verified.

	I5-8500B									
2	Cisco Meraki	N/A	N/A	N/A	Router	N/A	192.168.128.1	e0:cb:bc:40:5c:90	N/A	Manually set and verified.
3	Peer 1	Kali Linux, Rasbian	acumensec/acumensec, root/toor	2019.4, 3.2.6	TLS Webserver, OCSP Responder	TLS 1.2/HTTPS	10.1.2.160 10.1.9.12	00:0c:29:5b:a8:35 08:00:27:f3:a5:86	OpenSSl 1.1.1d, Acumen-tlsc v3.6, XCA v2.1.2, Wireshark v2.6.8, tcpdump v4.9.3, x509-mod v1.1 (in-house tool)	Manually set and verified.
4	Peer 2	Kali Linux	Root/toor	2019.4	DNS server	TLS 1.2/HTTPS	10.1.2.109	00:0c:29:dc:44:8a	Wireshark v2.6.8, Apache webserver v 2.4.43	Manually set and verified.
6	Peer 3	Rasbian	Root/toor	3.2.6	Bridge	TLS1.2/HTTPS	???	08:00:27:f3:a5:86	Tcpdump v4.9.3, Acumen-tlsc v3.6	Manually set and verified.
7	Apple Update Server	N/A	N/A	N/A	Update Server	TLSv1.2/HTTPS	23.202.149.132	N/A	N/A	NA
		Packet captures are performed on Peer 1, Peer 2, Peer 3. Time was manually set and verified on all above identified devices. The TOE is automatically synchronized with Apple Time servers.								

Table 6: Configuration Information for Intel Core i5-8500B (Coffee Lake i5)

5.1.2. Test Bed for Intel Core i7-1060NG7 (Ice Lake i7):

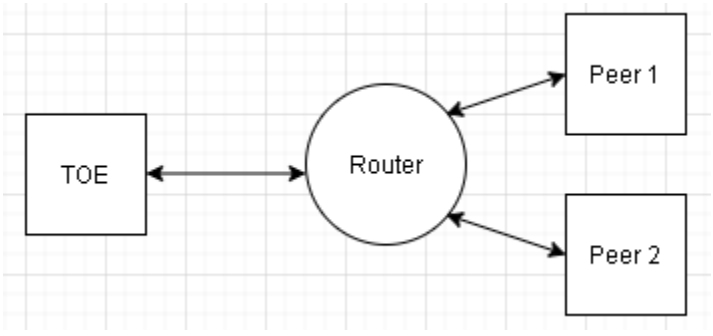

Figure 5: Testbed #1 for Icelake i7

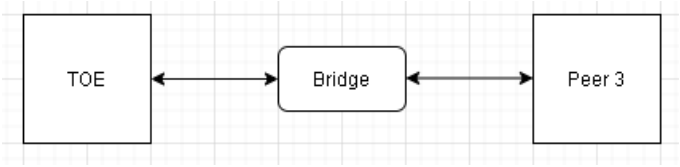

Figure 6: Testbed #2 for Icelake i7

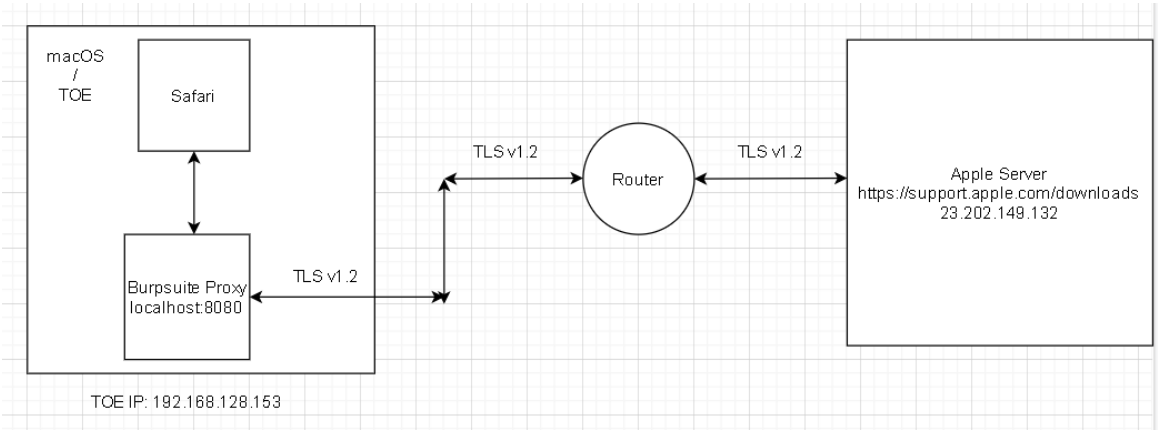

Figure 7: Test Bed #3 for Icelake i7 FPT_TUD_EXT.1.1 and FPT_TUD_EXT.2.1

Sr. No	Name	OS	Credentials	Version	Function	Protocols	IP address	MAC Address	Tools (version)	Time
1	Icelake-i7-Macbook Air	Apple macOS Catalina	acumensec/ acumensec	10.15.5	TOE	TLS 1.2/HTTPS	192.168.128.153	3c:22:fb:7a:10:12	Safari 13.0.5 Proxy-BurpSuite Pro v2020.2	Manually set and verified
2	Peer 1	Ubuntu	Acumensec/ 123TesT321	18.04.4	Test VM	TLS 1,2 HTTPS	10.1.2.169	00:0c:29:80:d5:84	Acumen-tlsc v3.2, XCA v1.4.1 Wireshark v2.6.10, x509-mod v1.1	Manually set and verified
3	Peer 2	Kali Linux	Root/toor	2019.4	DNS server	TLS 1.2/HTTPS	10.1.2.109	00:0c:29:dc:44:8a	Wireshark v2.6.8, Apache webserver v 2.4.43	Manually set and verified
4	Peer 3	Rasbian	Root/toor	3.2.6	Bridge	TLS1.2/HTTPS		08:00:27:f3:a5:86	Tcpdump v4.9.3, Acumen-tlsc v3.6	Manually set and verified
5	Cisco Meraki	N/A	N/A	N/A	Router	N/A	192.168.128.1	e0:cb:bc:40:5c:90	N/A	Manually set and verified

6	Apple Update Server	N/A	N/A	N/A	Update Server	TLSv1.2/HTTPS	23.202.149.132	N/A	N/A	N/A

Table 7: Configuration Information for Intel Core i7-1060NG7 (Ice Lake i7)

5.2 Test Time/Location

All testing was carried at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from 11/19 to 08/20.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept with the evaluator.

6 Detailed Test Cases (Auditing)

6.1 Test Cases

6.1.1 FAU_GEN.1 Guidance 1

The evaluator will check the administrative guide and ensure that it lists all of the auditable events. The evaluator will check to make sure that every audit event type selected in the ST is included.	
Evaluator Findings	The evaluator examined the guidance document to determine if it lists all auditable events. The section 14 titled "Auditing" of the AGD was used to determine the verdict of this assurance activity. The evaluator compared the list of events to the auditable events listed in the Protection Profile for Operating Systems, Version 4.2.1 [GPOSPP] and found that all of the auditable events selected in the ST are included. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.2 FAU_GEN.1 Test 1

Item	Data/Description
Test ID	FAU_GEN.1_T1
Objective	The evaluator will test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. This should include all instance types of an event specified. When verifying the test results, the evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.
Test Flow	• Trigger each auditable event on the TOE. • Verify that each audit record is generated and contains the required information.
Pass/Fail Explanation	The TOE generates the appropriate audit logs.

Result	Pass. The TOE generates the appropriate audit logs that match the format specified in the administrative guide and the fields in each audit record provide the required information

6.1.3

6.1.4 FAU_GEN.1.2 Guidance 1

The evaluator will check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator will ensure that the fields contains the information required.	
Evaluator Findings	The evaluator examined the guidance document 'Apple macOS Catalina 10.15 Common Criteria Configuration Guide' to determine if it provides a format for audit records. Section 14 titled "Auditing" of the AGD was used to determine the verdict of this assurance activity. The evaluator found that the administrative guide provides a format for audit records and each audit record format type is covered. Upon investigation, the evaluator also found that there is a brief description of each field and that the fields contain the information required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.5 FAU_GEN.1.2 Test 1

Item	Data/Description
Test ID	FAU_GEN.1.2_T1
Objective	The evaluator will test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. The evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.
Pass/Fail Explanation	Test satisfied by FAU_GEN.1.1 Test 1.
Result	Pass.

6.1.6 FCS_CKM.1 TSS 1

The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.	
Evaluator Findings	The evaluator examined the TSS to determine if it identifies the key sizes supported by the TOE. The TSS entry for FCS_CKM.1 in the section 7 titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states "The TOE supports RSA key sizes of 2048 bits, and 3072 bits for key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. RSA keys are used for TLS sessions.

	The TOE acts as sender and receiver in the RSA key establishment scheme. The TOE supports Elliptical NIST curve sizes of P-256, P-384 and P-521 for key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4. The Elliptic keys are used in support of ECDH key exchange. ECDH public and private keys are used for Diffie-Hellman key establishment for TLS communications". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.7 FCS_CKM.1 Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP.	
Evaluator Findings	The evaluator examined guidance documentation "Apple macOS Catalina 10.15 Common Criteria Configuration Guide" to determine if it instructs the administrator how to configure TOE to use the selected key generation schemes and key sizes. Upon investigation, the evaluator found Section 8 "Configuring TLS" of the AGD mentions that no configuration is required for generating keys for TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.8 FCS_CKM.1 Test 1

The evaluator shall verify the implementation of Key Generation by the TOE using the Key Generation test.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the appropriate FIPS 186-4 Key Generation tests. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate numbers are listed below.
CAVP Algorithm Certificate	RSA Certs : A8, A22, A26, A27, A30, A33, A34 ECDSA Certs : A8, A22, A26, A27, A30, A33, A34
Verdict	Pass.

6.1.9 FCS_CKM.2 TSS 1

The evaluator will ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator will examine the TSS to verify that it identifies the usage for each scheme.

Evaluator Findings	The evaluator examined the TSS to determine if the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. The TSS entries for FCS_CKM.1 and FCS_CKM.2 in Section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator compared the key establishment schemes listed in FCS_CKM.2 to the key generation schemes listed in FCS_CKM.1. Upon investigation, the evaluator found that FCS_CKM.2 does not introduce any key generation scheme not included in FCS_CKM.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.10 FCS_CKM.2 Guidance 1

The evaluator will verify that the AGD guidance instructs the administrator how to configure the OS to use the selected key establishment scheme(s).	
Evaluator Findings	The evaluator examined the guidance documentation "Apple macOS Catalina 10.15 Common Criteria Configuration Guide" to determine if it instructs the administrator how to configure TOE to use the selected key establishment schemes. Upon investigation, the evaluator found that Section 8 "Configuring TLS" of the AGD mentions that no configuration is necessary for TLS key establishment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.11 FCS_CKM.2 Test 1

The evaluator shall verify the implementation of the key establishment schemes supported by the TOE using the applicable tests.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the SP 800-56B Key Agreement Scheme tests. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate numbers are listed below.
CAVP Algorithm Certificate	KAS-ECC Cert: A8
Verdict	Pass.

6.1.12 FCS_CKM_EXT.4 TSS 1

The evaluator examines the TSS to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

Evaluator Findings	The evaluator examined the TSS to ensure that it describes how keys are managed in volatile memory, along with details of how each identified key is introduced into volatile memory. The TSS entries for FCS_CKM_EXT.4 in the section 7 titled 'TOE Summary Specification' was used to determine the verdict of this assurance activity. The evaluator found that the TSS states that the TOE includes a Keychain Access program that allows users the ability to add, remove, and manage certificates and private keys. Persistent keys are introduced into volatile memory after decryption or unwrapping and are also destroyed by a single overwrite consisting of zeroes. Ephemeral cryptographic keys are destroyed by a single overwrite consisting of zeroes. Based on these findings this assurance activity is considered satisfied.
Verdict	Pass

6.1.13 FCS_CKM_EXT.4 TSS 2

The evaluator will check to ensure the TSS lists each type of key that is stored in in non-volatile memory, and identifies how the TOE interacts with the underlying platform to manage keys (e.g., store, retrieve, destroy). The description includes details on the method of how the TOE interacts with the platform, including an identification and description of the interfaces it uses to manage keys (e.g., file system APIs, platform key store APIs).	
Evaluator Findings	The evaluator examined the TSS to ensure that it lists each type of key that is stored in non-volatile memory and whether it identifies how the TOE interacts with the underlying platform to manage the keys. The TSS entry for FCS_CKM_EXT.4 in Section 7 "TOE Summary Specification" was used to determine the verdict of this assurance activity. The evaluator found that the TSS states that the TOE includes a Keychain Access program that allows users the ability to add, remove, and manage certificates and private keys. Keys stored in non-volatile memory are destroyed by a single overwrite consisting of zeros. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.14 FCS_CKM_EXT.4 TSS 3

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator will verify that the pattern does not contain any CSPs.	
Evaluator Findings	The evaluator found that the ST does not make use of open assignment.
Verdict	Pass.

6.1.15 FCS_CKM_EXT.4 TSS 4

The evaluator will check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.	
Evaluator Findings	The TSS does not identify any configurations or circumstances that may not strictly conform to the key destruction requirement.
Verdict	Pass

6.1.16 FCS_CKM_EXT.4 Guidance 1

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator will check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information.	
Evaluator Findings	The evaluator checked whether the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. Section 19 “Key Destruction” of the AGD was used to determine the verdict of this assurance activity. The AGD mentions that “There are no circumstances that do not conform to the key destruction requirement (e.g. sudden unexpected power loss).” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.17 FCS_CKM_EXT.4 Guidance 2

The evaluator will check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible.	
Evaluator Findings	The evaluator checked whether the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible. Section 19 “Key Destruction” of the AGD was used to determine the verdict of this assurance activity. The AGD mentions that all keys are erased when the host device is powered off, during reboot, when a user locks or logs off the host device, the TOE detects the configured inactivity time has passed and the host device logs out, or when the host device is put to sleep. Once the keys are no longer required, the key that was used to perform the specific operation is erased from volatile memory by performing a single overwrite of zeroes. The erase operation is performed by the SEP and is not configurable by a user. There are no circumstances that do not conform to the key destruction requirement (e.g. sudden unexpected power loss).

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.18 FCS_CKM_EXT.4 Test 1

Item	Data/Description
Test ID	FCS_CKM_EXT.4_T1
Objective	Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator will: 1. Record the value of the key in the TOE subject to clearing. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1. 3. Cause the TOE to clear the key. 4. Cause the TOE to stop the execution but not exit. 5. Cause the TOE to dump the entire memory of the TOE into a binary file. 6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1. Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.
Note	The TOE uses different Class keys within T2 SEP. The evaluator has provided an explanation corresponding to each class key and its' availability as below: Apple developer access is required to conduct this test. The TOE automatically clears the key depending on the key class. E.g. Class A key is available only when the TOE is unlocked and the same Class A key and any Class A

Class Key#	Internal	Availability
1	A	When Unlocked
2	B	While Locked
3	C	After First Unlock
4	D	macOS does not have Class D key. Class D key is only present in Apple iOS.
5	E	Unused
6	AK	When unlocked
7	CK	After first unlock
8	DK	Always
9	AKU	When unlocked
10	CKU	After first unlock
11	DKU	Always
12	APKU	N/A (Passcode enabled)

	key variations (e.g. AK, AKU etc) are cleared by the TOE whenever the user locks the TOE or the TOE transitions into a sleep mode.
Test Flow	• Record the values of all the class keys within the T2 SEP and dump the class keys. • Cause the TOE to clear the keys, • Cause the TOE to dump the entire memory of the TOE into a binary file. • Search the content of the binary file created in Step #5 for instances of the known key value from Step #1. • Ensure that complete keys do not exist anywhere in volatile memory
Pass/Fail Explanation	Pass. The TOE correctly clears the TLS Session keys, T2 SEP keys - class A, class AK, class AKU, and class APKU from the SEP. The evaluator ensured that the complete Class A, class AK, class, AKU, and class APKU keys do not exist anywhere in volatile memory. This meets testing requirements.
Result	Pass.

6.1.19 FCS_CKM_EXT.4 Test 2

Item	Data/Description
Test ID	FCS_CKM_EXT.4_T2
Objective	Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator will use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended. 1. Identify the purpose of the key and what access should fail when it is deleted. 2. (e.g. the data encryption key being deleted would cause data decryption to fail.) 3. Cause the TOE to clear the key. 4. Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.
Test Flow	• Configure the correct reference identifier on TOE: https://test.acusec.com • Start TLS webserver connection and verify the TOE successfully connects to the server. • Remove the Root CA certificate from the TOE keychain. • Attempt to connect from the TOE to the Server and verify the connection fails. • Verify that the TOE deletes the Keychain Password when it is no longer needed.
Pass/Fail Explanation	Pass. The TOE correctly clears the keys held in non-volatile memory.
Result	Pass.

6.1.20 FCS_CKM_EXT.4 Test 3

Item	Data/Description
Test ID	FCS_CKM_EXT.4_T3

Objective	Test 3: The following tests apply only to selection a), since the TOE in this instance has more visibility into what is happening within the underlying platform (e.g., a logical view of the media). In selection b), the TOE has no visibility into the inner workings and completely relies on the underlying platform, so there is no reason to test the TOE beyond test 2. For selection a), the following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern. Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media (e.g., MBR file system): 1. Record the value of the key in the TOE subject to clearing . 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1. 3. Cause the TOE to clear the key . 4. Search the logical view that the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails. TD0365 applied. TD can be found at: https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0365
Pass/Fail Explanation	Pass. This test is performed in conjunction with FCS_CKM_EXT.4 Test #2. The TOE correctly clears the keys held in non-volatile memory.

6.1.21 FCS_CKM_EXT.4 Test 4

Item	Data/Description
Test ID	FCS_CKM_EXT.4_T4
Objective	Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media: 1. Record the logical storage location of the key in the TOE subject to clearing. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1. 3. Cause the TOE to clear the key. 4. Read the logical storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized. The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.
Pass/Fail Explanation	Pass. This test is performed in conjunction with FCS_CKM_EXT.4 Test #2. The TOE correctly clears the keys held in non-volatile memory.

6.1.22 FCS_COP.1(1) Guidance 1

The evaluator shall verify that the AGD documents contains instructions required to configure the OS to use the required modes and key sizes.	
Evaluator Findings	The evaluator examined the guidance documentation to determine if any configuration is required to be done to configure the functionality for the required modes and key sizes is present. Upon investigation, the evaluator found that Section 8 “Configuring TLS” of the AGD indicates that no key configuration is necessary for TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.23 FCS_COP.1(1) Test 1

The evaluator shall verify the implementation of symmetric encryption supported by the TOE.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the Encryption test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below. Based on these findings, this activity is considered satisfied.
CAVP Algorithm Certificate	AES Certs: AES-CBC : 128 & 256 bit - A7, A8, A11, A15 A19, A20, A21, A23, A24, A25 AES-GCM : 128 & 256 bit - A7, A8, A10, A13, A21, A28, A31
Verdict	Pass.

6.1.24 FCS_COP.1(2) TSS 1

The evaluator shall check that the association of the hash function with other application cryptographic functions (for example, the digital signature verification function) is documented in the TSS.	
Evaluator Findings	The evaluator examined the TSS to determine that the association of the hash function with other TSF cryptographic features is documented in the TSS. The TSS entry for FCS_COP.1(2) in section 7 ‘TOE Summary Specification’ of the ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes each of the associated TSF cryptographic functions for which hashing is associated with, as follows: The TSS states: “The TOE supports Cryptographic hashing services conforming to FIPS PUB 180-4. The hashing algorithms are used for signature services and HMAC services.

	The following hashing algorithms supported: SHA-1, SHA-256, SHA-384 and SHA-512. The message digest sizes supported are: 160 bits, 256 bits, 384 bits and 512 bits." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.25 FCS_COP.1(2) Guidance 1

The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.	
Evaluator Findings	The evaluator checked the AGD document to determine that any configuration that is required to configure the required hash sizes is present. Section 9 "TOE Cryptographic Operation – Hashing, Encryption and Decryption" was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the AGD states "The TOE supports Cryptographic hashing services conforming to FIPS PUB 180-4. The hashing algorithms are used for signature services and HMAC services. The following hashing algorithms supported: SHA-1, SHA-256, SHA-384 and SHA-512. The message digest sizes supported are: 160 bits, 256 bits, 384 bits and 512 bits. Note: By default, the TOE supports the hash sizes. The TOE does not allow the user to configure the hash size." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.26 FCS_COP.1(2) Test 1

The evaluator shall verify the implementation of hashing supported by the TOE.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the Hashing test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.
CAVP Algorithm Certificate	SHS Certs: SHA-1, SHA-256, SHA-384, SHA-512 - A8, A22, A27, A29, A33, A30, A26, A32, A34
Verdict	Pass.

6.1.27 FCS_COP.1(3) Test 1

The evaluator shall verify the implementation of the digital signature algorithms supported by the TOE.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the Digital Signature test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below. Based on these findings, this activity is considered satisfied.
CAVP Algorithm Certificate	RSA 2048-bit and 3072-bit SigGen and SigVer – A8, A22, A26, A27, A30, A34 ECDSA - A8, A22, A26, A27, A30, A34
Verdict	Pass.

6.1.28 FCS_COP.1(4) Test 1

The evaluator shall verify the implementation of HMAC supported by the TOE.	
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the HMAC test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.
CAVP Algorithm Certificate	HMAC Certs: SHA-1, SHA-256, SHA-384, SHA-512 - A8, A22, A27, A29, A33, A30, A26, A32, A34
Verdict	Pass.

6.1.29 FCS_RBG_EXT.1.1 Test 1

Item	Data/Description
Test ID	FCS_RBG_EXT.1.1_T1
Objective	The evaluator will perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator will perform 15 trials for each configuration. The evaluator will also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality. If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator will generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A).

	If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator will generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.
Evaluator Findings	The implemented cryptographic module employed by the TOE has been subject to the DRBG tests. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.
CAVP Algorithm Certificate	• CTR-DRBG (AES-128 and AES-256) : A7, A8, A10, A21, A31 (CoreCrypto User) A23, A15, A13, A28 (CoreCrypto Kernel)
Verdict	Pass.

6.1.30 FCS_STO_EXT.1.1 TSS 1

The evaluator will check the TSS to ensure that it lists all persistent sensitive data for which the OS provides a storage capability. For each of these items, the evaluator will confirm that the TSS lists for what purpose it can be used, and how it is stored. The evaluator will confirm that cryptographic operations used to protect the data occur as specified in FCS_COP.1(1).

Evaluator Findings	The evaluator examined the TSS to ensure that it lists all persistent sensitive data for which the OS provides a storage capability. The TSS entry for FCS_STO_EXT.1 in the section 7 titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. The TSS states that the TOE stores the following sensitive data: • Usernames and passwords used for authentication. • Trusted Certificates for TLS sessions. • Private Keys used for TLS session. macOS offers a repository, called Keychain, that conveniently and securely stores user names and passwords, including digital identities, encryption keys, and secure notes. It can be accessed by opening the Keychain Access app in /Applications/Utilities/. Using a keychain eliminates the requirement to enter—or even remember—the credentials for each resource. An initial default keychain is created for each Mac user, though users can create other keychains for specific purposes. In addition to user keychains, macOS relies on a number of system-level keychains that maintain authentication assets that aren't user-specific, such as network credentials and public key infrastructure (PKI) identities. Keychain items are encrypted using two different AES-256-GCM keys: a table key (metadata), and a per-row key (secret-key). Keychain metadata (all attributes other than kSecValue) is encrypted with the metadata key to speed searches while the secret value (kSecValueData) is encrypted with the secret-key. The meta-data key is protected by the Secure Enclave, but is cached in the application processor to allow fast queries of the keychain.
Verdict	Pass

6.1.31 FCS_STO_EXT.1.1 Guidance 1

The evaluator will also consult the developer documentation to verify that an interface exists for applications to securely store credentials.	
Evaluator Findings	The evaluator examined the guidance document to verify that an interface exists for applications to securely store credentials. The section 16 titled "Access Control Policy" of the AGD was used to determine the verdict of this assurance activity. The evaluator verified that an interface exists for applications to securely store credentials. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.32 FCS_TLSC_EXT.1.1 TSS 1

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component.	
Evaluator Findings	The evaluator examined the TSS to ensure that the cipher suites supported are specified. The TSS entry for FCS_TLSC_EXT.1 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the cipher suites supported by the TOE for TLS client connections. The following cipher suites are identified as supported within the TSS, • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 Next, the evaluator examined the definition of FCS_TLSC_EXT.1 in section 6.2.1.10 of the ST andthe evaluator found that the cipher suites for TLS client connection specified in the definition of the SFR are consistent with the description within the TSS of ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.33 FCS_TLSC_EXT.1.1 Guidance 1

The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.	
Evaluator Findings	The evaluator examined the guidance document to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. The section 8 titled " Configuring TLS" of the AGD was used to determine the verdict of this assurance activity. The evaluator found that the AGD mentions that no configuration is needed from the user for TLS. This section also specifies the cipher suites supported by the OS for TLS session establishments. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass.

6.1.34 FCS_TLSC_EXT.1.1 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T1
Objective	The evaluator shall establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Flow	• Establish a TLS connection with each of the claimed cipher suites and verify the connection is successful: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
Pass/Fail Explanation	Pass. The TOE connects to the server with the specified cipher suites.
Result	Pass

6.1.35 FCS_TLSC_EXT.1.1 Test 2

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T2
Objective	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Flow	• Establish a connection using a server certificate that contains the Server Authentication purpose in the EKU field. • Verify the connection is established. • Establish a connection using a server certificate that does not contain the Server Authentication purpose in the EKU field. • Verify the connection is not established.

Pass/Fail Explanation	Pass. The TOE does not allow a connection when the Server Authentication purpose in the EKU field is missing.
Result	Pass

6.1.36 FCS_TLSC_EXT.1.1 Test 3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T3
Objective	The evaluator will send a server certificate in the TLS connection that does not match the server-selected cipher suite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite or send a RSA certificate while using one of the ECDSA cipher suites.) The evaluator will verify that the OS disconnects after receiving the server's Certificate handshake message.
Test Flow	• Send a server certificate in the TLS connection that does not match the server-selected cipher suite. (ECDHE-ECDSA-AES128-SHA) • Verify the connection is not successful.
Pass/Fail Explanation	Pass. The TOE does not permit a connection when the server certificate does not match the server-selected cipher suite.
Result	Pass

6.1.37 FCS_TLSC_EXT.1.1 Test 4

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T4
Objective	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.
Test Flow	• Configure the server for the TLS_NULL_WITH_NULL_NULL cipher suite. • Attempt to connect to the server from the TOE and verify the connection was not successful.
Pass/Fail Explanation	Pass. The TOE does not connect to a server when the TLS_NULL_WITH_NULL_NULL cipher suite is configured.
Result	Pass

6.1.38 FCS_TLSC_EXT.1.1 Test 5.1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.1
Objective	Test 5: The evaluator will perform the following modifications to the traffic: Test 5.1: Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection.
Test Flow	• Change the TLS version on the server to a non-supported TLS version using acumen-tlsc tool. (SSL v3.0) • Verify the TOE rejects the connection.
Pass/Fail Explanation	Pass. The TOE does not allow a connection when the TLS version on the server is a non-supported TLS version.

Result	Pass

6.1.39 FCS_TLSC_EXT.1.1 Test 5.2

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.2
Objective	Test 5.2: Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE cipher suite) or that the server denies the client's Finished handshake message.
Note	The evaluator used an in-house tool- acumentlsc v2.1 to execute this test. This is a proprietary tool developed by Acumen for Acumen.
Test Flow	Attempt a connection to a remote server that modifies the server's nonce in the server hello message. Show the TOE rejects the connection.
Pass/Fail Explanation	Pass. The TOE rejects a connection to a remote server after receiving an invalid server nonce.
Result	Pass

6.1.40 FCS_TLSC_EXT.1.1 Test 5.3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.3
Objective	Test 5.3: Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator will verify that the client rejects the connection after receiving the Server Hello.
Test Flow	• Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. • Verify the TOE rejects the connection.
Pass/Fail Explanation	Pass. The TOE does not allow a connection to be made when the server's selected cipher suite in the Server Hello handshake message is a cipher suite not presented in the Client Hello handshake message.
Result	Pass

6.1.41 FCS_TLSC_EXT.1.1 Test 5.4

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.4
Objective	Test 5.4 (conditional): If an ECDHE or DHE cipher suite is selected, modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message.
Note	The evaluator used an in-house tool- acumentlsc v2.1 to execute this test. This is a proprietary tool developed by Acumen for Acumen.

Test Flow	• Attempt a connection to a remote server that will run a tool allowing the modification of the signature block on the server key exchange. • Show the TOE rejects the server key exchange message.
Pass/Fail Explanation	Pass. The TOE rejects a connection to a server after receiving an invalid signature from the server.
Result	Pass

6.1.42 FCS_TLSC_EXT.1.1 Test 5.5

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.5
Objective	Test 5.5: Modify a byte in the Server Finished handshake message and verify that the client sends a fatal alert upon receipt and does not send any application data.
Note	The evaluator used an in-house tool- acumentlsc v2.1 to execute this test. This is a proprietary tool developed by Acumen for Acumen.
Test Flow	• Attempt a connection to a remote server that will run a tool allowing the modification of server finished message. • Show the TOE rejects the server key exchange message.
Pass/Fail Explanation	Pass. The TOE does not all a connection to proceed when a byte in the Server Finished handshake message has been modified.
Result	Pass

6.1.43 FCS_TLSC_EXT.1.1 Test 5.6

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5.6
Objective	Test 5.6: Send a garbled message from the Server after the Server has issued the Change Cipher Spec message and verify that the client denies the connection.
Test Flow	• Attempt a connection to a remote server that sends a garbled message after the Change Cipher Spec. • Show the TOE rejects the connection.
Pass/Fail Explanation	Pass. The TOE does not allow a connection to proceed when a garbled message from the Server is sent after the Server has issued the Change Cipher Spec message.
Result	Pass

6.1.44 FCS_TLSC_EXT.1.2 TSS 1

The evaluator will ensure that the TSS describes the client's method of establishing all reference identifiers from the application-configured reference identifier, including which types of reference identifiers are supported (e.g. Common Name, DNS Name, URI Name, Service Name, or other application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator will ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the OS.	
Evaluator Findings	The evaluator checked the TSS to determine if it describes the client's method of establishing reference identifiers. The TSS entry for

	FCS_TLSC_EXT.1 in the section 7 titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes the client's method of establishing reference identifiers. Specifically, the TSS states the following, "The macOS Catalina verifies that the presented identifier matches the reference identifier according to RFC 6125. The reference identifiers supported are DNS and IP addresses. The TOE does not support certificate pinning. Wild cards are supported". Based on these findings, this Assurance Activity is considered satisfied.
Verdict	Pass

6.1.45 FCS_TLSC_EXT.1.2 Guidance 1

The evaluator will verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.	
Evaluator Findings	The evaluator examined the guidance document to verify that it includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS. The section 15 titled "Reference Identifiers" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the AGD states that "The TOE verifies that the presented identifier matches the reference identifier according to RFC 6125. The reference identifiers supported are DNS and IP addresses. The TOE does not support certificate pinning. Wild cards are supported." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.46 FCS_TLSC_EXT.1.2 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T1
Objective	The evaluator will present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator will verify that the connection fails.
Test Flow	• Configure the CN and SAN of the server certificate to contain values that do not match the reference identifier. • Connect from the TOE (client) to the server and verify the connection was not successful.
Pass/Fail Explanation	Pass. The TOE did not allow the connection to proceed.
Result	Pass

6.1.47 FCS_TLSC_EXT.1.2 Test 2

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T2

Objective	The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type.
Test Flow	• Present a server certificate that contains a valid CN (10.1.9.12) but invalid SAN (10.1.8.12). • Verify the connection fails. • Present a server certificate that contains a valid CN (test.acumen.com) but invalid SAN (test.acu.com). • Verify the connection fails.
Pass/Fail Explanation	Pass. The TOE does not allow a connection when the server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier.
Result	Pass

6.1.48 FCS_TLSC_EXT.1.2 Test 3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T3
Objective	Test 3 [conditional]: If the TOE does not mandate the presence of the SAN extension, the evaluator will present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator will verify that the connection succeeds. If the TOE mandates the presence of the SAN extension, this Test shall be omitted.
Pass/Fail Explanation	The TOE mandates the presence of the SAN extension. This test is thereby omitted.

6.1.49 FCS_TLSC_EXT.1.2 Test 4

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T4
Objective	• Present a server certificate that contains a bad CN (10.2.9.12) and a good SAN (10.1.9.12). • Verify the connection succeeds. • Present a server certificate that contains a bad CN (not.acusec.com) and a good SAN (test.acusec.com). • Verify the connection succeeds.
Test Flow	•
Pass/Fail Explanation	Pass. The TOE successfully connects when the server certificate contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches.
Result	Pass

6.1.50 FCS_TLSC_EXT.1.2 Test 5.1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T5.1
Objective	The evaluator will perform the following wildcard tests with each supported type of reference identifier: Test 5.1: The evaluator will present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Flow	• Attempt a connection to a remote TLS server using a wildcard not in the left-most label (foo.*.acusec.com) • Show the TOE rejects the connection.
Pass/Fail Explanation	Pass. The TOE rejects a connection to a remote server using an invalid wildcard.
Result	Pass.

6.1.51 FCS_TLSC_EXT.1.2 Test 5.2

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T5.2
Objective	The evaluator will present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g.*.example.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator will configure the reference identifier without a leftmost label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.
Test Flow	• Attempt a connection to a remote TLS server using a certificate. with a wildcard in the left-most label with the reference identifier set to a single left-most label (*.acusec.com, test.acusec.com) • Show the connection succeeds. • Change the reference identifier to not have any leftmost label and attempt to connect to the same TLS server (*.acusec.com, acusec.com) • Show the connection fails. • Change the reference identifier to have 2 leftmost labels and attempt to connect to the same TLS server (*.acusec.com, foo.test.acusec.com) • Show the connection fails.
Pass/Fail Explanation	Pass. The TOE behaves as expected when receiving a server certificate using a wildcard matching the reference identifier label.
Result	Pass.

6.1.52 FCS_TLSC_EXT.1.2 Test 5.3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T5.3

Objective	The evaluator will present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.
Test Flow	• Attempt a connection to a remote TLS server using a certificate with a wildcard preceding the public suffix and with the reference identifier set to a single left-most label (*.com, acusec.com) • Show the connection fails. • Change the reference identifier to not have 2 leftmost labels and attempt to connect to the same TLS server (*.com test.acusec.com) • Show the connection fails.
Pass/Fail Explanation	Pass. The TOE rejects a connection to a server using a certificate with a wildcard preceding the public suffix.
Result	Pass.

6.1.53 FCS_TLSC_EXT.1.2 Test 6

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T6
Objective	[conditional] If URI or Service name reference identifiers are supported, the evaluator will configure the DNS name and the service identifier. The evaluator will present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator will repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.
Pass/Fail Explanation	URI Names and Service names are unsupported. This test is Not Applicable.

6.1.54 FCS_TLSC_EXT.1.3 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT_1_3_T1
Objective	The evaluator will demonstrate that a peer using a certificate without a valid certification path results in an authenticate failure. Using the administrative guidance, the evaluator will then load the trusted CA certificate(s) needed to validate the peer's certificate and demonstrate that the connection succeeds. The evaluator then shall delete one of the CA certificates and show that the connection fails.
Pass/Fail Explanation	Pass. This test is covered by FIA_X509_EXT.1.1 Test #1.

6.1.55 FCS_TLSC_EXT.1.3 Test 2

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.3_T2

Objective	The evaluator will demonstrate that a peer using a certificate which has been revoked results in an authentication failure.
Pass/Fail Explanation	Pass. This test is performed in conjunction with FIA_X509_EXT.1.1 Test#3. The TOE fails to establish a connection with a revoked server certificate. This meets testing requirements.

6.1.56 FCS_TLSC_EXT.1.3 Test 3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.3_T3
Objective	The evaluator will demonstrate that a peer using a certificate which has passed its expiration date results in an authentication failure.
Pass/Fail Explanation	Pass. This test is covered by FIA_X509_EXT.1.1 Test #2

6.1.57 FCS_TLSC_EXT.1.3 Test 4

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.3_T4
Objective	the evaluator will demonstrate that a peer using a certificate which does not have a valid identifier shall result in an authentication failure.
Pass/Fail Explanation	Pass. This test is covered by FCS_TLSC_EXT.1.2 Test 1-5.3

6.1.58 FCS_TLSC_EXT.2.1 TSS 1

The evaluator will verify that the TSS describes support for the Supported Groups Extension and whether the required behavior is performed by default or may be configured.	
Evaluator Findings	The evaluator verified that TSS describes support for the Supported Groups Extension and whether the required behaviour is performed by default or may be configured. The TSS entry for FCS_TLSC_EXT.2 in the section 7 titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS provides full details regarding the TOE support for ECDH parameters, as follows, "The TOE, by default, presents the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: secp256r1, secp384r1, and secp521r1." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.59 FCS_TLSC_EXT.2.1 Guidance 1

If the TSS indicates that support for the Supported Groups Extension must be configured to meet the requirement, the evaluator will verify that AGD guidance includes configuration instructions for the Supported Groups Extension.

Evaluator Findings	The evaluator examined the guidance document to verify that AGD guidance includes configuration of the supported Elliptic Curves Extension. The section 8 titled "Configuring TLS" of the AGD was used to determine the verdict of this assurance activity. The evaluator found that the AGD states The TOE supports the following NIST Elliptic Curves in the Client Hello. No configuration is needed from the user. • Secp256r1 • Secp384r1 • Secp521r1 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.60 FCS_TLSC_EXT.2.1 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT_2_1_T1
Objective	The evaluator will configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.
Test Flow	• Attempt a connection to a remote TLS server using secp256r1 and verify the TOE accepts the connection. • Verify with packet capture. • Attempt a connection to a remote TLS server using secp384r1 and verify the TOE accepts the connection. • Verify with packet capture. • Attempt a connection to a remote TLS server using secp521r1 and verify the TOE accepts the connection. • Verify with packet capture.
Pass/Fail Explanation	Pass. The TOE accepts a connection using each of the claimed curves.
Result	Pass

6.1.61 FCS_TLSC_EXT.4 TSS 1

Objective	The evaluator will ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the FCS_TLSC_EXT.4 in the section 7 titled "TOE Summary Specification" in the Security Target to verify that the TSS includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that the TOE uses X.509v3 certificates for performing mutual authentication for TLS in HTTPS connections. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.62 FCS_TLSC_EXT.4 Guidance 1

Objective	The evaluator will verify that the AGD guidance required per FIA_X509_EXT.2.1 includes instructions for configuring the client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled section 8.1 titled "Configure the TOE for TLS Mutual Authentication in the AGD to verify that it includes instructions for configuring the client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the AGD states that the user can configure the TOE for mutual authentication as described below: • Obtain a TLS Client certificate. • Install the TLS Client Certificate on the TOE Keychain. • Establish a connection with the TLS webserver that requests the TLS Client certificate. • During the TLS handshake, the TOE will prompt the user to enter their account password. This password proves as the authorization factor to use the TLS Client certificate. • After entering the correct password in the password prompt, the TOE will use its' TLS Client certificate to authenticate itself to the TLS webserver. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.1.63 FCS_TLSC_EXT.4 Test 1

Item	Data/Description
Test ID	FCS_TLSC_EXT.4.1_T1
Objective	The evaluator will establish a connection to a peer server that is not configured for mutual authentication (i.e. does not send Server's Certificate Request (type 13) message). The evaluator observes negotiation of a TLS channel and confirms that the TOE did not send Client's Certificate message (type 11) during handshake.
Pass/Fail Explanation	Pass. This test case is completed in conjunction with all the FCS_TLSC_EXT.1 test cases. In each test case, the TOE did not present a certificate per the server connection.

6.1.64 FCS_TLSC_EXT.4 Test 2

Item	Data/Description

Test ID	FCS_TLSC_EXT.4.1_T2
Objective	The evaluator will establish a connection to a peer server with a shared trusted root that is configured for mutual authentication (i.e. it sends Server's Certificate Request (type 13) message). The evaluator observes negotiation of a TLS channel and confirms that the TOE responds with a non-empty Client's Certificate message (type 11) and Certificate Verify (type 15) messages.
Pass/Fail Explanation	Pass. This test case is completed in conjunction with FIA_X509_EXT.2 test case 1. In this test case, the TOE presented a certificate per the server connection.

6.2 Test Cases (User Data Protection)

6.2.1 FDP_ACF_EXT.1.1 TSS 1

The evaluator will confirm that the TSS comprehensively describes the access control policy enforced by the OS. The description must include the rules by which accesses to particular files and directories are determined for particular users. The evaluator will inspect the TSS to ensure that it describes the access control rules in such detail that given any possible scenario between a user and a file governed by the OS the access control decision is unambiguous.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes the access control policy enforced by the OS and whether the description includes the rules by which accesses to particular files and directories are determined for particular users. The TSS entry for FDP_ACF_EXT.1 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, "The Apple File System (APFS) is the default file system for macOS Catalina and it provides access control to data in macOS Catalina. File system object attributes includes manipulation of metadata (e.g. change, access, modify time), as well as owner and permission data (e.g. group-ids for allowing multiple users to have the same access privileges, user-ids for individual access privileges, and permissions that can be assigned per user or group). These filesystem object attributes are based on the file system security schemes supported by macOS. macOS provides three file system security schemes: UNIX (BSD) permissions, POSIX access control lists (ACLs), and sandbox entitlements. In addition, the BSD layer provides several per-file flags that override UNIX permissions. These schemes are described in the sections that follow. • Unix (BSD) Permissions • POSIX access control lists • sandbox entitlements macOS allows admin users to disable ownership and permissions checking for removable volumes on a per-volume basis by choosing Get

	Info on the volume in Finder, then checking the “Ignore ownership on this volume” checkbox. Also the evaluator found that the TSS describes the permissions for each of the schemes and access control rules in such detail that given any possible scenario between a user and a file governed by the OS the access control decision is unambiguous. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2.2 FDP_ACF_EXT.1.1 Test 1

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T1
Objective	The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to read the file created in the first user's home directory. The evaluator will ensure that the read attempt is denied.
Test Flow	• Create two standard user accounts on the system. • Create a file within the first user’s home directory. • Log off the first user’s account. • Log in as the second user. • Attempt to read the file created in the first user’s home directory. • Verify the read attempt is denied.
Pass/Fail Explanation	Pass. The second user is unable to access the files of the first user. This meets the testing requirement.
Result	Pass

6.2.3 FDP_ACF_EXT.1.1 Test 2

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T2
Objective	The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification is denied.
Test Flow	• Create two standard user accounts on the system. • Create a file within the first user’s home directory. • Log off the system. • Log in as the second user. • Attempt to modify the file created in the first user’s home directory. • Verify the modify attempt is denied.

Pass/Fail Explanation	Pass. The second user is unable to modify the files of the first user. This meets the testing requirement.
Result	Pass

6.2.4 FDP_ACF_EXT.1.1 Test 3

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T3
Objective	The evaluator will authenticate to the system as the first user and create a file within that user's user directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to delete the file created in the first user's home directory. The evaluator will ensure that the deletion is denied.
Test Flow	• Create two standard user accounts on the system. • Create a file within the first user's home directory. • Log off the system. • Log in as the second user. • Attempt to delete the file created in the first user's home directory. • Verify the delete attempt is denied.
Pass/Fail Explanation	Pass. The second user is unable to delete the file of the first user. This meets the testing requirement.
Result	Pass

6.2.5 FDP_ACF_EXT.1.1 Test 4

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T4
Objective	The evaluator will authenticate to the system as the first user. The evaluator will attempt to create a file in the second user's home directory. The evaluator will ensure that the creation of the file is denied.
Test Flow	• Create two standard user accounts on the system. • Attempt to create a file in second user's home directory. • Execute terminal commands • Ensure that the file creation is denied.
Pass/Fail Explanation	Pass. The first user was unable to create files in the home directory of the second user. This meets the testing requirement.
Result	Pass

6.2.6 FDP_ACF_EXT.1.1 Test 5

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T5
Objective	The evaluator will authenticate to the system as the first user and attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification of the file is accepted.

Test Flow	• Create two standard user accounts on the system. • Attempt to modify a file in the first user's home directory. • Verify the attempt is accepted.
Pass/Fail Explanation	Pass. The first user is able to modify files in the directory of the first user. This meets the testing requirement.
Result	Pass

6.2.7 FDP_ACF_EXT.1.1 Test 6

Item	Data/Description
Test ID	FDP_ACF_EXT.1.1_T6
Objective	The evaluator will authenticate to the system as the first user and attempt to delete the file created in the first user's directory. The evaluator will ensure that the deletion of the file is accepted.
Test Flow	• Create two standard user accounts on the system. • Attempt to delete a file in the first user's home directory. • Verify the attempt is accepted.
Pass/Fail Explanation	Pass. The first user is able to delete files in the directory of the first user. This meets the testing requirement.
Result	Pass.

6.3 Test Cases (Identification and Authentication)

6.3.1 FIA_AFL.1.1 Test 1

Item	Data/Description
Test ID	FIA_AFL.1.1_T1
Objective	The evaluator will set an administrator-configurable threshold for failed attempts, or note the ST-specified assignment. The evaluator will then (per selection) repeatedly attempt to authenticate with an incorrect password, PIN, or certificate until the number of attempts reaches the threshold. Note that the authentication attempts and lockouts must also be logged as specified in FAU_GEN.1.
Test Flow	• Set an administrator-configurable threshold (3) for failed attempts. • Attempt to login as user1 with incorrect password for 3 times. • Verify authentication failure using audit logs. • Verify user1 account locked out due to failed attempts
Pass/Fail Explanation	Pass. The TOE behaves as configured when a user makes multiple invalid login attempts. This meets the testing requirement.
Result	Pass

6.3.2 FIA_AFL.1.2 Test 1

Item	Data/Description
Test ID	FIA_AFL.1.2_T1

Objective	The evaluator will attempt to authenticate repeatedly to the system with a known bad password. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail Explanation	Pass. Test Covered by FIA_AFL.1.1.. The TOE behaves as configured when a user makes multiple invalid login attempts.

6.3.3 FIA_AFL.1.2 Test 2

Item	Data/Description
Test ID	FIA_AFL.1.2_T2
Objective	The evaluator will attempt to authenticate repeatedly to the system with a known bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail Explanation	This test is Not Applicable. The TOE only supports username and password for FIA_AFL_EXT.1.
Result	NA

6.3.4 FIA_AFL.1.2 Test 3

Item	Data/Description
Test ID	FIA_AFL.1.2_T3
Objective	The evaluator will attempt to authenticate repeatedly to the system using both a bad password and a bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail Explanation	This test is Not Applicable. The TOE only supports username and password for FIA_AFL_EXT.1.
Result	NA

6.3.5 FIA_UAU.5.1 Test 1 (Known Username & Password)

Item	Data/Description
Test ID	FIA_UAU.5.1_T1
Objective	If user name and password authentication is selected, the evaluator will configure the OS with a known user name and password and conduct the following tests: Test 1: The evaluator will attempt to authenticate to the OS using the known user name and password. The evaluator will ensure that the authentication attempt is successful.

Test Flow	• Attempt to login with correct username/password (user1/123TesT321) • Verify the authentication attempt is successful using audit logs.
Pass/Fail Explanation	Pass. The TOE allows users to authenticate with a valid username and password. This meets the testing requirement.
Result	Pass

6.3.6 FIA_UAU.5.1 Test 2 (Known Username & Incorrect Password)

Item	Data/Description
Test ID	FIA_UAU.5.1_T2
Objective	If user name and password authentication is selected, the evaluator will configure the OS with a known user name and password and conduct the following tests: Test 2: The evaluator will attempt to authenticate to the OS using the known user name but an incorrect password. The evaluator will ensure that the authentication attempt is unsuccessful.
Test Flow	• Attempt to login with correct username but incorrect password (user1/321TesT123) • Verify the authentication attempt is unsuccessful using audit logs.
Pass/Fail Explanation	Pass. The TOE denies access to a user using a valid username with an invalid password. This meets the testing requirement.
Result	Pass

6.3.7 FIA_UAU.5.1 Test 1 (Known Username & PIN)

Item	Data/Description
Test ID	FIA_UAU.5.1_T1
Objective	If user name and PIN that releases an asymmetric key is selected, the evaluator will examine the TSS for guidance on supported protected storage and will then configure the TOE or OE to establish a PIN which enables release of the asymmetric key from the protected storage (such as a TPM, a hardware token, or isolated execution environment) with which the OS can interface. The evaluator will then conduct the following tests: Test 1: The evaluator will attempt to authenticate to the OS using the known user name and PIN. The evaluator will ensure that the authentication attempt is successful.
Test Flow	• Attempt to authenticate to the TOE using known username (in this case “cert”) and PIN (in this case 123456) • Verify the authentication attempt is successful.
Pass/Fail Explanation	Pass. The TOE successfully authenticates the user when a known username and PIN is used to authenticate.
Result	Pass

6.3.8 FIA_UAU.5.1 Test 2 (Known Username & Incorrect PIN)

Item	Data/Description
Test ID	FIA_UAU.5.1_T2

Objective	If user name and PIN that releases an asymmetric key is selected, the evaluator will examine the TSS for guidance on supported protected storage and will then configure the TOE or OE to establish a PIN which enables release of the asymmetric key from the protected storage (such as a TPM, a hardware token, or isolated execution environment) with which the OS can interface. The evaluator will then conduct the following tests: Test 2: The evaluator will attempt to authenticate to the OS using the known user name but an incorrect PIN. The evaluator will ensure that the authentication attempt is unsuccessful.
Test Flow	• Attempt to authenticate to the TOE using known username (in this case "cert") and incorrect PIN (in this case 1234567) • Verify the authentication attempt is not successful.
Pass/Fail Explanation	Pass. The TOE fails to authenticate the user when a known username and an incorrect PIN is used to authenticate.
Result	Pass

6.3.9 FIA_UAU.5.2 TSS 1

The evaluator will ensure that the TSS describes each mechanism provided to support user authentication and the rules describing how the authentication mechanism(s) provide authentication.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes each mechanism provided to support user authentication and the rules describing how the authentication mechanism(s) provide authentication. The TSS entry for FIA_UAU.5.2 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, "The TOE supports authentication based on username and password and smart cards. For password-based authentication, the user account contains a username and a password. A random salt is created for the password in a Password-Based Derivation Key Function 2 (PBKDF2) with SHA-512. This result is then stored in the Directory Services node. When a user logs into the system, the TOE uses the entered password and the randomly generated salt and compares this with the stored value. If they match, then the user is granted access to the system. If the values do not match, then the user is not granted access. Smart card authentication provides a strong two-factor authentication in macOS Catalina. This requires the user to have a username and a PIN. The user initially logins in providing a valid username and password. Once successfully authenticated, a smart card is paired to the user account. When the smart card pairing is initiated, the user is required to enter the smart card's PIN to unlock the card. The PIN is not stored by the TOE. The

	TOE then passes the entered PIN to the smart card for verification. Upon successful verification, the smart card's certificate (which contains its public key) is sent to the TOE for storage. The certificate is associated with the user's account and the card is considered to be paired with the user. When a user inserts a Smart Card into the host platform, the user enters the associated PIN to unlock the card. Once unlocked, a signing operation is performed by the card. The TOE verifies the signature using the paired certificate for authentication." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.3.10 FIA_UAU.5.2 Guidance 1

The evaluator will verify that configuration guidance for each authentication mechanism is addressed in the AGD guidance.	
Evaluator Findings	The evaluator examined the guidance documentation to verify that configuration guidance for each authentication mechanism is addressed. Section 18 "Authorization Factors" of the AGD was used to determine the verdict of this Assurance Activity. The evaluator found that the AGD specifies that the TOE supports password and external smart card authentication factors and addresses both the authentication mechanisms. Hence each authentication mechanism is addressed in the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.3.11 FIA_UAU.5.2 Test 1 (Known Username & Password, Known Username & PIN)

Item	Data/Description
Test ID	FIA_UAU.5.2_T1
Objective	For each authentication mechanism selected, the evaluator will enable that mechanism and verify that it can be used to authenticate the user at the specified authentication factor interfaces.
Pass/Fail Explanation	Pass. This test is performed in conjunction with FIA_UAU.5.1 Test #1 (Known Username & Password) and FIA_UAU.5.1 Test #1 (Known Username & PIN). The evaluator verified that the TOE successfully authenticates the user with the specified authentication factors - Known Username & Password and Known Username & PIN.
Result	Pass

6.3.12 FIA_UAU.5.2 Test 2 (Known Username & Password, Known Username & PIN), (Known Username & Incorrect Password, Known Username & Incorrect PIN)

Item	Data/Description
Test ID	FIA_UAU.5.2_T2
Objective	For each authentication mechanism rule, the evaluator will ensure that the authentication mechanism(s) behave as documented in the TSS.
Pass/Fail Explanation	Pass. This test is performed in conjunction with FIA_UAU.5.1 Test #1 (Known Username & Password) and FIA_UAU.5.1 Test #1 (Known Username & PIN) and FIA_UAU.5.1 Test #2 (Known Username & Incorrect Password) and FIA_UAU.5.1 Test #2 (Known Username & Incorrect PIN). The evaluator verified that the TOE successfully authenticates the user with the specified authentication factors - Known Username & Password and Known Username & PIN. The evaluator also verified that the TOE fails to authenticate the user with the specified authentication factors - Known Username & Incorrect Password and Known Username & Incorrect PIN. This behavior is documented in the TSS.
Result	Pass.

6.3.13 FIA_X509_EXT.1.1 TSS 1

The evaluator will ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.	
Evaluator Findings	The evaluator examined the TSS to determine where certificate validation occurs and that the TSS also provides a description of the certificate path validation algorithm. The TSS entry for FIA_X509_EXT.1 under section 7 titled 'TOE Summary Specification' reveals: "When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certificate path validation. • The certificate path must terminate with a trusted CA certificate. • The OS shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates. The OS shall validate the extendedKeyUsage field according to the following rules: • Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. • Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

	• Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. • S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field. • OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field. (Conditional) Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field. X509 certificates are validated when imported into the TOE's trusted certificate store, during session establishment with a peer and prior to presenting a certificate to the peer during trusted channel implementation using TLS for mutual authentications." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.3.14 FIA_X509_EXT.1.1 Test 1

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T1
Objective	The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: • by establishing a certificate path in which one of the issuing certificates is not a CA certificate, • by omitting the basicConstraints field in one of the issuing certificates, • by setting the basicConstraints field in an issuing certificate to have CA=False, • by omitting the CA signing bit of the key usage field in an issuing certificate, and • by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails. ***TD0525 applied***
Test Flow	Omitting the basicConstraints field in one of the issuing certificates.

	• Generate a chain of 4 certificates with one of the certificates missing basicConstraints field. • Install ca-chain on the TOE • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails. • Verify the connection with Packet capture. --- The basicConstraints field in an issuing certificate to have CA=False. • Generate a chain of 4 certificates with one of the certificates have CA=False. • Install ca-chain on the TOE • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails. • Verify the connection with Packet capture. --- Omitting the CA signing bit of the key usage field in an issuing certificate. • Generate a chain of 4 certificates with certificates missing CA signing bit of the key usage field in an issuing certificate. • Install ca-chain on the TOE • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails. • Verify the connection with Packet capture. --- Setting the path length field of a valid CA field to a value strictly less than the certificate path. • Generate a chain of 4 certificates with certificates have CA field to a value strictly less than the certificate path. • Install ca-chain on the TOE • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails. • Verify the connection with Packet capture. --- Establish a valid certificate path consisting of valid CA certificates and remove trust in one of the CA certificates and verify connection succeeded and failed respectively. • The evaluator generated a chain of 4 certificates. • Rootca_x5091.1_t1->ica1->ica2->server • Import and manually trust the certificate chain of Rootca_x5091.1_t1->ica1 on the TOE System keychain. Note the absence of ica2 from the TOE System keychain. • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails. • Load the missing ica2 certificate on the TOE keychain. • Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection is successful. • Delete ica2 certificate from the TOE System keychain

	• Attempt a connection from the TOE with the OpenSSL server (10.1.2.160) and verify the connection fails.
Pass/Fail Explanation	Pass. The TOE will not validate a certificate with an incomplete path or missing basicConstraints or missing CA signing bit or having CA=False, but it will accept that same certificate when it has the full CA chain with all mandatory fields inside the certificate defined.
Result	Pass.

6.3.15 FIA_X509_EXT.1.1 Test 2

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T2
Objective	The evaluator will demonstrate that validating an expired certificate results in the function failing.
Test Flow	• The evaluator generated a chain of 4 certificates. • CAroot->ICA>ICA2->10.1.2.169_expired • Import and manually trust the certificate chain of CAroot->ICA>ICA2 on the TOE System keychain. • Attempt a connection from the TOE with the OpenSSL server (10.1.2.169) and verify the connection fails.
Pass/Fail Explanation	Pass. The evaluator verified that validating an expired certificate resulted in function failing. This meets the testing requirements.
Result	Pass

6.3.16 FIA_X509_EXT.1.1 Test 3

Item	Data/Description
Test ID	FIA_X509_EXT_1_1_T3
Objective	The evaluator will test that the OS can properly handle revoked certificates - conditional on whether CRL, OCSP, OCSP stapling, or OCSP multi-stapling is selected; if multiple methods are selected, then a test shall be performed for each method. The evaluator will test revocation of the node certificate and revocation of the intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA). If OCSP stapling per RFC 6066 is the only supported revocation method, testing revocation of the intermediate CA certificate is omitted. The evaluator will ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. ***TD0525 applied***
Test Flow	• OCSP Stapling- For valid Leaf Certificate: Start the TLS webserver and observe the connection attempt from the TOE succeeds

	• OCSP Stapling- For revoked Leaf Certificate: Start the TLS webserver and observe the connection attempt from the TOE failed
Pass/Fail Explanation	Pass. The TOE fails to establish a connection with a revoked server certificate. The TOE successfully establishes the connection with a valid server certificate. This meets testing requirements.
Result	Pass

6.3.17 FIA_X509_EXT.1.1 Test 4

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T4
Objective	If any OCSP option is selected, the evaluator shall configure the OCSP server or use a man-in-the middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set, and verify that validation of the CRL fails. ***TD0525 applied***
Test Flow	• Configure OCSP responder with a certificate without the OCSP signing purpose • Start the TLS webserver and observe the connection attempt from the TOE • The TOE will ignore the OCSP responder response because the response is not signed with a certificate that with the OCSP signing purpose • The TOE will complete the connection
Pass/Fail Explanation	Pass. When the TOE receives an OCSP response without the signing purpose, the TOE rejects the OCSP response and completes the connection. This meets the testing requirements.
Result	Pass/Fail

6.3.18 FIA_X509_EXT.1.1 Test 5

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T5
Objective	The evaluator will modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate should fail to parse correctly.)
Test Flow	• Attempt a connection to a remote modified TLS server using acumen-tlsc tool that would perform the necessary modification on the server certificate. Verify that the TOE rejects the connection: • Verify that the connection fails with packet capture. • Verify with the help of logs.

Pass/Fail Explanation	The TOE denies the connection to a remote TLS server when the server certificate has been modified. This meets the testing requirement.
Result	Pass

6.3.19 FIA_X509_EXT.1.1 Test 6

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T6
Objective	The evaluator will modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate should not validate.)
Test Flow	• Attempt a connection to a remote server running a tool that would allow sending a modified leaf certificate. • Show the TOE denies the connection.
Pass/Fail Explanation	Pass. The TOE denies the connection to a remote TLS server when the server certificate has been modified. This meets the testing requirement.
Result	Pass

6.3.20 FIA_X509_EXT.1.1 Test 7

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T7
Objective	The evaluator will modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate should not validate.)
Test Flow	• Attempt a connection to a remote server running a tool that would allow sending a modified leaf certificate. • Show the TOE denies the connection.
Pass/Fail Explanation	The TOE denies the connection to a remote TLS server when the server certificate has been modified. This meets the testing requirement.
Result	Pass

6.3.21 FIA_X509_EXT.1.1 Test 8a

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T8a
Objective	Test 8a: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.
Test Flow	• Create a certificate chain with three certificates using EC curves. • Add only the RootCA on the TOE. • Attempt a connection from a remote server and verify that it is successful. • Verify the connection with packet capture.

Pass/Fail Explanation	Pass. The TOE validates the certificate chain when the ec parameter certificate chain is used. This meets the testing requirement.
Result	Pass

6.3.22 FIA_X509_EXT.1.1 Test 8b

Item	Data/Description
Test ID	FIA_X509_EXT.1.1_T8b
Objective	Test 8b: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall replace the intermediate certificate in the certificate chain for Test 8a with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8a, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.
Test Flow	• Replace the ICA in the earlier test with a modified certificate and signed by the trusted RootCA. • Attempt a connection from the remote server and verify that it fails. • Verify the failed connection with a packet capture.
Pass/Fail Explanation	Pass. The TOE rejects a connection when the ICA certificate has been modified. This meets the testing requirement.
Result	Pass

6.3.23 FIA_X509_EXT.1.2 Test 1

Item	Data/Description
Test ID	FIA_X509_EXT.1.2_T1
Objective	The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Pass/Fail Explanation	Pass. Covered in FIA_X509_EXT.1.1 Test #1, as the TOE will not validate a certificate with missing basicConstraints inside an issuer's certificate, but it will accept that same certificate when it has the full CA chain with the basicConstraints field defined in the issuing certificates.
Result	Pass.

6.3.24 FIA_X509_EXT.1.2 Test 2

Item	Data/Description
Test ID	FIA_X509_EXT.1.2_T2
Objective	The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension not set. The validation of the certificate path fails.
Pass/Fail Explanation	Pass. Covered in FIA_X509_EXT.1.1 Test #1 as the TOE will not validate a certificate with missing CA flag inside an issuer's certificate, but it will accept that same

	certificate when it has the full CA chain with the CA flag set inside the issuing certificates.
Result	Pass.

6.3.25 FIA_X509_EXT.1.2 Test 3

Item	Data/Description
Test ID	FIA_X509_EXT.1.2_T3
Objective	The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.
Pass/Fail Explanation	Pass. Covered in FIA_X509_EXT.1.1 Test #1 as the TOE validated a full CA chain with a certificate which has CA flag set inside an issuer's certificate and connection succeeded.
Result	Pass.

6.3.26 FIA_X509_EXT.2.1 Test 1

Item	Data/Description
Test ID	FIA_X509_EXT.2.1_T1
Objective	The evaluator will acquire or develop an application that uses the OS TLS mechanism with an X.509v3 certificate. The evaluator will then run the application and ensure that the provided certificate is used to authenticate the connection. The evaluator will repeat the activity for any other selections listed.
Test Flow	• Acquire an application (macOS Safari in this case) that uses OS TLS mechanism with x509v3 certificate • Run the application and ensure that the provided certificate is used to authenticate the connection.
Pass/Fail Explanation	Pass. The application successfully leverages the OS TLS mechanism for authentication using x509v3 certificate.
Result	Pass.

6.4 Test Cases (Security Management)

6.4.1 FMT_MOF_EXT.1 TSS 1

The evaluator will verify that the TSS describes those management functions that are restricted to Administrators, including how the user is prevented from performing those functions, or not able to use any interfaces that allow access to that function.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes the management functions that are restricted to Administrators, including how the user is prevented from performing those functions, or not able to use any interfaces that allow access to that function. The TSS entry for FMT_MOF_EXT.1 & FMT_SMF_EXT.1 in

	the section 7 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. The TSS states that, The TOE supports the following roles: Administrator and User. The Administrator is a member of the local admin group whereas the User is not a member of the local group. The Administrator has access to the following management functions: • Enable/disable screen lock • Configure screen lock inactivity timeout • Configure local audit storage capacity • Configure minimum password Length • Configure minimum number of special characters in password • Configure minimum number of numeric characters in password • Configure minimum number of uppercase characters in password • Configure minimum number of lowercase characters in password • Configure lockout policy for unsuccessful authentication attempts through [limiting number of attempts during a time period] • Configure host-based firewall • Configure name/address of directory server with which to bind • Configure name/address of remote management server from which to receive management settings • Configure name/address of audit/logging server to which to send audit/logging records • Configure audit rules • Configure name/address of network time server • Enable/disable automatic software update • Configure WiFi interface • Enable/disable Bluetooth interface The user has access to the following management functions: • Enable/disable screen lock

	• Configure screen lock inactivity timeout • Enable/disable Bluetooth interface Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.4.2 FMT_MOF_EXT.1 Test 1

Item	Data/Description
Test ID	FMT_MOF_EXT.1_T1
Objective	For each function that is indicated as restricted to the administrator, the evaluation shall perform the function as an administrator, as specified in the Operational Guidance, and determine that it has the expected effect as outlined by the Operational Guidance and the SFR. The evaluator will then perform the function (or otherwise attempt to access the function) as a non- administrator and observe that they are unable to invoke that functionality.

Test Flow	• Enable/disable [screen lock]
	  ○ Navigate to System Preferences -> Security & Privacy -> Verify the screen is locked
	  ○ Navigate to System Preferences-> Security & Privacy-> Click on “Click the lock to make changes”. Then enter credentials to unlock the screen.
	• Configure [screen lock] inactivity timeout
	  ○ Navigate to System Preferences -> Security & Privacy
	  ○ Then change the setting from Immediately to 15 minutes from the Drop-down list.
	• Configure local audit storage capacity
	  ○ Navigate to /etc/security
	  ○ Execute command: nano audit_control
	• Configure minimum password length
	  ○ Execute commands:
	  ▪ pwpolicy getaccountpolicies > temp.xml
	  ▪ vi temp.xml
	  ▪ pwpolicy setaccountpolicies temp.xml
	• Configure minimum number of special characters in password
	  ○ Execute commands:
	  ▪ pwpolicy getaccountpolicies > temp.xml
	  ▪ vi temp.xml
	  ▪ pwpolicy setaccountpolicies temp.xml
	• Configure minimum number of numeric characters in password
	  ○ Execute commands:
	  ▪ pwpolicy getaccountpolicies > temp.xml
	  ▪ vi temp.xml
	  ▪ pwpolicy setaccountpolicies temp.xml

	• Configure minimum number of uppercase characters in password
	  ○ Execute commands:
	  ▪ pwpolicy getaccountpolicies > temp.xml
	  ▪ vi temp.xml
	  ▪ pwpolicy setaccountpolicies temp.xml
	• Configure minimum number of lowercase characters in password
	  ○ Execute commands:
	  ▪ pwpolicy getaccountpolicies > temp.xml
	  ▪ vi temp.xml
	  ▪ pwpolicy setaccountpolicies temp.xml
	• Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts]
	  ○ Execute command: pwpolicy -u user_1 -set policy “maxFailedLoginAttempts=3”
	• Configure host-based firewall
	  ○ Navigate to System Preferences -> Security & Privacy -> Firewall -> Turn On/Off firewall
	• Configure name/address of audit/logging server to which to send audit/logging records
	  ○ Navigate to /etc/
	  ○ Execute: nano syslog.conf
	  ○ Enter the IP address and port number to which to send the audit records.
	• Configure audit rules
	  ○ Navigate to /etc/security
	  ○ Execute command: nano audit_control
	• Configure name/address of network time server
	  ○ Execute command: /usr/sbin/systemsetup -setnetworktimeserver “time.euro.apple.com”
	  ○ Execute command: /usr/sbin/systemsetup -setusingnetworktime on
	• Enable/disable automatic software update
	  ○ To enable execute command: softwareupdate –schedule on
	  ○ To disable execute command: softwareupdate –schedule off
	• Configure Wifi interface
	  ○ Navigate to System Preferences -> Network -> Create a new WiFi Test Network
	• Enable/Disable Bluetooth interface
	  ○ Navigate to System Preferences -> Bluetooth- > Turn On/Off Bluetooth

Management Function	Administrator	User
Enable/disable [screen lock]	X	X
Configure [screen lock] inactivity timeout	X	X
Configure local audit storage capacity	X	-
Configure minimum password Length	X	-
Configure minimum number of special characters in password	X	-
Configure minimum number of numeric characters in password	X	-
Configure minimum number of uppercase characters in password	X	-
Configure minimum number of lowercase characters in password	X	-
Configure lockout policy for unsuccessful authentication attempts through [*limiting number of attempts during a time period]*	X	-
Configure host-based firewall	X	-
Configure name/address of directory server with which to bind	-	-
Configure name/address of remote management server from which to receive management settings	-	-
Configure name/address of audit/logging server to which to send audit/logging records	X	-

		Configure audit rules	X	-	
		Configure name/address of network time server	X	-	
		Enable/disable automatic software update	X	-	
		Configure WiFi interface	X	-	
		Enable/disable Bluetooth interface	X	X	
		Enable/disable [*no other external interfaces]*	-	-	
		[no other management functions]	-	-	
Pass/Fail Explanation	Pass. The TOE restricts configuration changes to privileged users. This meets the testing requirement.				
Result	Pass.				

6.4.3 FMT_SMF_EXT.1.1 Guidance 1

The evaluator will verify that every management function captured in the ST is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.	
Evaluator Findings	The evaluator verified that the guidance documentation provides information required to perform the management duties associated with the management function. Section 3.2 “TOE Management Functions” of the AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that, the guide states that the TOE supports the following roles: Administrator and User. A user can Enable/disable screen lock, Configure screen lock inactivity timeout and Enable/disable Bluetooth interface. Section 3.2 of the AGD contains information required to perform the management duties associated with the management function such as Enable/Disable Screen Lock, Configure screen-lock inactivity timeout, Configure local audit storage capacity, Configure minimum password length, Configure minimum number of special characters in password, Configure minimum number of numeric characters in password, Configure minimum number of uppercase characters in password, Configure minimum number of lowercase characters in password, Configure lockout policy for unsuccessful authentication attempts through, Configure host-based firewall, Configure name/address of audit/logging server to which to send audit/logging records, Configure audit rules, Configure name/address of network time server, Enable/disable automatic software update, Configure WiFi interface and Enable/disable Bluetooth interface. Based on these findings, this Assurance activity is considered satisfied.
Verdict	Pass.

6.4.4 FMT_SMF_EXT.1.1 Test 1

Item	Data/Description
Test ID	FMT_SMF_EXT.1.1_T1
Objective	The evaluator will test the OS's ability to provide the management functions by configuring the operating system and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Pass/Fail Explanation	Pass. FMT_SMF_EXT.1.1 Specification of Management Functions requirements have been met throughout the various security functionality testing of the TOE.
Result	Pass.

6.5 Test Cases (Protection of the TSF)

6.5.1 FPT_ACF_EXT.1.1 TSS 1

The evaluator will confirm that the TSS specifies the locations of kernel drivers/modules, security audit logs, shared libraries, system executables, and system configuration . Every file does not need to be individually identified, but the system's conventions for storing and protecting such files must be specified.	
Evaluator Findings	The evaluator examined the TSS to ensure that it identifies the locations of kernel drivers/modules, security audit logs, shared libraries, system executables, and system configuration files. The TSS entry for FPT_ACF_EXT.1 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, "The TOE provides access control policy through the system integrity protection. This technology prevents from malicious software from modifying files and folders. The System Integrity program restricts the root user account (an administrator superuser account) and limits the actions that the root user can perform on protected parts of the Mac operating system. System Integrity Protection includes protection for these parts of the system: /System /usr /bin /sbin /var Apps that are pre-installed with macOS Catalina Kernel drivers and modules: -/System/Library/Extensions/ Security audit logs: -/var/audit/* Shared libraries: -/Library/Frameworks/ -/Library/PrivateFrameworks/ -/System/Library/Frameworks/

	-/System/Library/PrivateFrameworks/ System executables: -/Applications System configuration files: -System-wide “preferences” -/Library/Preferences/ -User-specific “preferences” -/Users/<username>/Library/Preferences Security Audit Logs: -/etc/security/audit-control System-wide local directory services credentials: -/private/var/db/dslocal/nodes/Default/ System Integrity Protection is designed to allow modification of these protected parts only by processes that are signed by Apple and have special entitlements to write to system files, such as Apple software updates and Apple installers. Apps that you download from the Mac App Store already work with System Integrity Protection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6.5.2 FPT_ACF_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T1
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 1: The evaluator will attempt to modify all kernel drivers and modules.
Test Flow	• Create an unprivileged user account. • Using the above account, attempt to modify all kernel drivers and modules. • Verify that the TOE denies this attempt.
Pass/Fail Explanation	Pass. The TOE does not allow an unprivileged user to modify kernel drivers and modules. This meets the testing requirement.
Result	Pass

6.5.3

6.5.4 FPT_ACF_EXT.1.1 Test 2

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T2

Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): The evaluator will attempt to modify all security audit logs generated by the logging subsystem.
Test Flow	• Create an unprivileged user account. • Using the above account, attempt to modify all security audit logs generated by the logging subsystem. • Verify that the TOE denies this attempt.
Pass/Fail Explanation	Pass. The TOE does not allow an unprivileged user to modify security audit logs. This meets the testing requirement.
Result	Pass

6.5.5 FPT_ACF_EXT.1.1 Test 3

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T3
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 3: The evaluator will attempt to modify all shared libraries that are used throughout the system.
Test Flow	• Create an unprivileged user account. • Using the above account, attempt to modify all shared libraries that are used throughout the system. • Verify that the TOE denies this attempt.
Pass/Fail Explanation	Pass. The TOE does not allow an unprivileged user to modify any shared libraries. This meets the testing requirement.
Result	Pass.

6.5.6 FPT_ACF_EXT.1.1 Test 4

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T4
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 4: The evaluator will attempt to modify all system executables.
Test Flow	• Create an unprivileged user account. • Using the above account, attempt to modify all security audit logs generated by the logging subsystem. • Verify that the TOE denies this attempt.
Pass/Fail Explanation	Pass. The TOE does not allow an unprivileged user to modify system executable. This meets the testing requirement.
Result	Pass.

6.5.7 FPT_ACF_EXT.1.1 Test 5

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T5
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 5: The evaluator will attempt to modify all system configuration files.
Test Flow	• Create an unprivileged user account. • Using the above account, attempt to modify all system configuration files on the TOE. • Verify that the TOE denies this attempt.
Pass/Fail Explanation	Pass. The TOE does not allow an unprivileged user to modify system configuration. This meets the testing requirement.
Result	Pass

6.5.8 FPT_ACF_EXT.1.1 Test 6

Item	Data/Description
Test ID	FPT_ACF_EXT.1.1_T6
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): The evaluator will attempt to modify any additional components selected.
Pass/Fail Explanation	No additional components have been selected. This test is Not Applicable.

6.5.9 FPT_ACF_EXT.1.2 Test 1

Item	Data/Description
Test ID	FPT_ACF_EXT.1.2 T1
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 1: The evaluator will attempt to read security audit logs generated by the auditing subsystem
Test Flow	• Create an unprivileged account • Using the unprivileged account attempt to read the security audit logs generated by the auditing subsystem. • Ensure that the the unprivileged user is unable to read the security audit logs.
Pass/Fail Explanation	Pass. The TOE prevents/denies an unprivileged user from reading security audit logs generated by the auditing subsystem on the TOE.
Result	Pass

6.5.10 FPT_ACF_EXT.1.2 Test 2

Item	Data/Description
Test ID	FPT_ACF_EXT.1.2 T2
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 2: The evaluator will attempt to read system-wide credential repositories
Test Flow	• Create an unprivileged account • Using the unprivileged account attempt to read system-wide credential repositories. • Ensure that the the unprivileged user is unable to read the system-wide credential repositories
Pass/Fail Explanation	Pass. The TOE prevents/denies an unprivileged user from system-wide credential repositories on the TOE.
Result	Pass

6.5.11 FPT_ACF_EXT.1.2 Test 3

Item	Data/Description
Test ID	FPT_ACF_EXT.1.2 T3
Objective	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): Test 3: The evaluator will attempt to read any other object specified in the assignment
Pass/Fail Explanation	No additional object is specified in the assignment. Hence this test is Not Applicable.
Result	NA

6.5.12 FPT_ASLR_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_ASLR_EXT.1.1_T1
Objective	The evaluator will select 3 executables included with the TSF. If the TSF includes a web browser it must be selected. If the TSF includes a mail client it must be selected. For each of these apps, the evaluator will launch the same executables on two separate instances of the OS on identical hardware and compare all memory mapping locations. The evaluator will ensure that no memory mappings are placed in the same location. If the rare chance occurs that two mappings are the same for a single executable and not the same for the other two, the evaluator will repeat the test with that executable to verify that in the second test the mappings are different. This test can also be completed on the same hardware and rebooting between application launches.

Test Flow	• Execute below steps twice for macOS Safari
	  ○ Start activity monitor and Select Safari.
	  ○ Send ABORT signal to crash the application

	○ Save the crash logs ○ Reboot machine. • Verify two instances of Safari do not share the same memory locations (Binary Images Address range). • Execute below steps twice for macOS Mail ○ Start activity monitor and Select Mail. ○ Send ABORT signal to crash the application ○ Save the crash logs ○ Reboot machine. • Verify two instances of Mail do not share the same memory locations (Binary Images Address range). • Execute below steps twice for macOS Facetime ○ Start activity monitor and Select Facetime. ○ Send ABORT signal to crash the application ○ Save the crash logs ○ Reboot machine. • Verify two instances of Facetime do not share the same memory locations (Binary Images Address range).
Pass/Fail Explanation	Pass. The TOE ensures that no memory mappings are placed in the same location. This meets the testing requirement.
Result	Pass

6.5.13 FPT_SBOP_EXT.1.1 TSS 1

For stack-based OSes, the evaluator will determine that the TSS contains a description of stack-based buffer overflow protections used by the OS. These are referred to by a variety of terms, such as stack cookie, stack guard, and stack canaries. The TSS must include a rationale for any binaries that are not protected in this manner.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains a description of stack-based buffer overflow protections used by the OS. The TSS entry for FPT_SBOP_EXT.1 in the section 7 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. The TSS states that, The macOS Catalina employs stack-based buffer overflow protections using address space layout randomization and non-executable stack and heap. The host platforms of the macOS Catalina support a feature called the NX bit which allows the operating system to mark certain parts of memory as non-executable. If the processor tries to execute code in any memory page marked as non-executable, the program will crash. The macOS Catalina takes leverages this feature by marking the stack and heap as non-executable. This makes buffer overflow attacks difficult because any attacks that places executable code on the stack or heap and then tries to execute that code will fail. The rational for all the binaries which are not protected by SBOP are the following: Type 1: The compiler can optimize away stack usage (which is certainly something macOS heavily rely on for performance reasons).

	Type 2: Some binaries are just small entry points that rely on system frameworks for all of their functionality. There, the binary itself is going to be really small (less than ~1000 instructions, sometimes as small as 10 instructions), so is much less likely to need stack protection. Type 3: There are very short program/functions that does not access the stack (and just forwards to system frameworks to do the real work) Type 4: There are tiny binaries with a single trivial function that does not need stack protections or tiny wrappers that does not make use of the stack. Type 5: Some binaries do not access the stack in any kind of vulnerable way. The TOE also randomizes process address memory location with 16 bit of entropy." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.5.14 FPT_SBOP_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_SBOP_EXT.1.1_T1
Objective	The evaluator will inventory the kernel, libraries, and application binaries to determine those that do not implement stack-based buffer overflow protections. This list should match up with the list provided in the TSS.
Test Flow	• The evaluator developed a script to execute this test and it is attached in execution output for reference. • The evaluator executed this script from the terminal with root privileges. • The evaluator then verified that the list of libraries that do not implement stack-based buffer overflow protection matches up with the list provided in the TSS.
Pass/Fail Explanation	Pass. The evaluator has analyzed the list of binaries not protected with the stack protector flag and has observed that the list matches with the ones described in the TSS section of the Security Target document. This meets testing requirements.
Result	Pass

6.5.15 FPT_TST_EXT.1.1 TSS 1

The evaluator will verify that the TSS section of the ST includes a comprehensive description of the boot procedures, including a description of the entire bootchain, for the TSF. The evaluator will ensure that the OS cryptographically verifies each piece of software it loads in the bootchain to include bootloaders and the kernel. Software loaded for execution directly by the platform (e.g. first-stage bootloaders) is out of scope. For each additional category of executable code verified before execution, the evaluator will verify that the description in the TSS describes how that software is cryptographically verified.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains description of the boot procedures, including a description of the entire bootchain, for the TSF.

	The TSS entry for FPT_TST_EXT.1 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, "When the OS boots with the T2 chip on, the chip executes code from read-only memory known as the Boot ROM. This immutable code, referred to as the hardware root of trust, is laid down during chip fabrication and is audited for vulnerabilities and implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the iBoot bootloader is signed by Apple's private key before allowing it to load. This is the first step in the chain of trust. iBoot verifies the kernel and kernel extension code on the T2 chip, which subsequently verifies the Intel UEFI firmware. The UEFI firmware and the associated signature are initially available only to the T2 chip. After verification, the UEFI firmware image is mapped into a portion of the T2 chip memory and this memory is made available to the (Intel) application processor via the enhanced Serial Peripheral Interface (eSPI). When the application processor first boots, it fetches the UEFI firmware via eSPI from the integrity-checked, memory-mapped copy of the firmware located on the T2 chip. The evaluation of the chain of trust continues on the application processor, with the UEFI firmware evaluating the signature for boot.efi, which is the macOS bootloader. The Intel-resident macOS secure boot signatures are stored in the same Image4 format used for iOS and T2 chip secure boot, and the code that parses the Image4 files is the same hardened code from the current iOS secure boot implementation. Boot.efi in turn verifies the signature of a new file called immutablekernel. When secure boot is enabled, the immutablekernel represents the complete set of Apple kernel extensions required to boot macOS. The secure boot policy terminates at the handoff to the immutablekernel, and after that, macOS security policies (such as System Integrity Protection and signed kernel extensions) take effect. Any errors or failures in this process result in Mac entering macOS Recovery mode, Apple T2 Security Chip recovery mode, or Apple T2 Security Chip DFU mode." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.5.16 FPT_TST_EXT.1.1 TSS 2

The evaluator will verify that the TSS contains a description of the protection afforded to the mechanism performing the cryptographic verification.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains a description of the protection afforded to the mechanism performing the cryptographic verification. The TSS entry for FPT_TST_EXT.1 in the section 7 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity.

	The TSS states that, "When the application processor first boots, it fetches the UEFI firmware via eSPI from the integrity-checked, memory-mapped copy of the firmware located on the T2 chip. The evaluation of the chain of trust continues on the application processor, with the UEFI firmware evaluating the signature for boot.efi, which is the macOS bootloader. The Intel-resident macOS secure boot signatures are stored in the same Image4 format used for iOS and T2 chip secure boot, and the code that parses the Image4 files is the same hardened code from the current iOS secure boot implementation. Boot.efi in turn verifies the signature of a new file called immutablekernel. When secure boot is enabled, the immutablekernel represents the complete set of Apple kernel extensions required to boot macOS. The secure boot policy terminates at the handoff to the immutablekernel, and after that, macOS security policies (such as System Integrity Protection and signed kernel extensions) take effect." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.5.17 FPT_TST_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_TST_EXT.1.1_T1
Objective	The evaluator will perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors and that the OS properly boots.
Test Flow	• Reboot TOE. • Execute command via TOE terminal and capture the boot log. • Verify after boot that the OS loaded properly and does not flag any integrity errors.
Pass/Fail Explanation	Pass. The TOE boots properly and does not show any integrity errors. This meets the testing requirement.
Result	Pass

6.5.18 FPT_TST_EXT.1.1 Test 2

Item	Data/Description
Test ID	FPT_TST_EXT.1.1_T2
Objective	The evaluator will modify a TSF executable that is part of the bootchain verified by the TSF (i.e. Not the first-stage bootloader) and attempt to boot. The evaluator will ensure that an integrity violation is triggered and the OS does not boot (Care must be taken so that the integrity violation is determined to be the cause of the failure to load the module, and not the fact that in such a way to invalidate the structure of the module).
Test Flow	• Modify the signature used to verify the Apple T2 Kernel. • Verify that the TOE detects the violation and fails to boot.
Pass/Fail Explanation	Pass. The TOE fails to boot when it detects an Integrity Violation. This meets the testing requirement.

Result	Pass

6.5.19

6.5.20 FPT_TST_EXT.1.1 Test 3

Item	Data/Description
Test ID	FPT_TST_EXT.1.1_T3
Objective	Test 3[conditional]: If the ST author indicates that the integrity verification is performed using a public key in an X509 certificate, the evaluator will verify that the boot integrity mechanism includes a certificate validation according to FIA_X509_EXT.1 for all certificates in the chain from the certificate used for boot integrity to a certificate in the trust store that are not themselves in the trust store. This means that, for each X509 certificate in this chain that is not a trust store element, the evaluator must ensure that revocation information is available to the TOE during the bootstrap mechanism (before the TOE becomes fully operational). ***TD0493 applied***
Note	TD 0493 Applied. https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0493
Pass/Fail Explanation	NA. The TOE does not use an X.509 certificate for integrity verification. The TOE uses digital signatures absent of an X.509 certificate

6.5.21 FPT_TUD_EXT.1.1 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.1.1_T1
Objective	The evaluator will check for an update using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require installing and temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update. The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1. If the signature verification is not performed as part of a trusted channel, the evaluator shall send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful ***TD0463 applied.***
Note	TD 0463 is applied. TD can be found at: https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0463

	By default, the TOE uses TLS v1.3 to establish a secure channel with Apple website and hence the TOE had to be configured to use a Proxy that limited the TLS version to TLS v1.2. Therefore, the user must configure a Proxy instance on the TOE that would restrict the TLS version to TLS v1.2.
Test Flow	• Configure a proxy instance on the TOE such as BurpSuite Pro v2020.2. (detailed steps included in Test Output) • Start macOS Safari to check for OS and Software Application updates. • Verify the TOE provides a list of available updates.
Pass/Fail Explanation	Pass. The TOE successfully establishes a secure channel with Apple website over TLS v1.2 by successfully validating its Server certificate. The TOE then shows/provides a list of available OS updates.
Result	Pass

6.5.22 FPT_TUD_EXT.1.2 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT_1.2_T1
Objective	The evaluator will ensure that the update has a digital signature belonging to the vendor prior to its installation. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
Test Flow	• The evaluator downloaded the OS update from https://support.apple.com/downloads (in this case macOSUpd10.15.6.dmg) • Verify the TOE software update has digital signature belonging to the vendor. • Modify the downloaded update in such a way that the digital signature is no longer valid. • Attempt to install the modified update. • Ensure that the TOE does not install the modified update.
Pass/Fail Explanation	Pass. The TOE rejects an update if the package has been modified. This meets the testing requirement.
Result	Pass.

6.5.23 FPT_TUD_EXT.1.2 Test 2

Item	Data/Description
Test ID	FPT_TUD_EXT.1.2_T2
Objective	The evaluator will ensure that the update has a digital signature belonging to the vendor. The evaluator will then attempt to install the update (or permit installation to continue). The evaluator will ensure that the OS successfully installs the update.
Test Flow	• Download the update from https://support.apple.com/downloads • Attempt to install the digitally signed update.

	• Ensure that the TOE installs the update.
Pass/Fail Explanation	Pass. An update with a valid digital signature was successfully installed on the TOE. This meets the testing requirement.
Result	Pass.

6.5.24

6.5.25 FPT_TUD_EXT.2.1 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.2.1_T1
Objective	The evaluator will check for updates to application software using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update. The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1. If the signature verification is not performed as part of a trusted channel, the evaluator shall send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful. ***TD0463 applied***
Note	TD 0463 applied. https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0463
Pass/Fail Explanation	Pass. This test is performed in conjunction with FPT_TUD_EXT.1 Test #1. The TOE successfully establishes a secure channel with Apple website over TLS v1.2 by successfully validating its Server certificate. The TOE then shows/provides a list of available software updates.
Result	Pass

6.5.26 FPT_TUD_EXT.2.2 Test 1

Item	Data/Description
Test ID	FPT_TUD_EXT.2.2_T1
Objective	The evaluator will ensure that the update has a digital signature which chains to the OS vendor or another trusted root managed through the OS. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
Test Flow	• The evaluator downloaded the application software update from https://support.apple.com/downloads (in this case ProVideoFormats.dmg) • Verify the application software update has a digital signature belonging to the vendor.

	• Modify the downloaded application software update in such a way that the digital signature is no longer valid. • Attempt to install the modified application software update. • Ensure that the TOE does not install the modified application software update.
Pass/Fail Explanation	Pass. The TOE won't allow an update to be installed with an invalid digital signature. This meets the testing requirement.
Result	Pass.

6.5.27

6.5.28 FPT_TUD_EXT.2.2 Test 2

Item	Data/Description
Test ID	FPT_TUD_EXT.2.2_T2
Objective	The evaluator will ensure that the update has a digital signature belonging to the OS vendor or another trusted root managed through the OS. The evaluator will then attempt to install the update. The evaluator will ensure that the OS successfully installs the update.
Test Flow	• Ensure the update has a valid digital signature • Attempt to install a valid update • Ensure that the TOE successfully installs the update
Pass/Fail Explanation	Pass. The TOE allows an update to be installed with a valid signature. This meets the testing requirement.
Result	Pass

6.6 Test Cases (TOE Access)

6.6.1 FTA_TAB.1.1 Test 1

Item	Data/Description
Test ID	FTA_TAB.1.1_T1
Objective	The evaluator will configure the OS, per instructions in the OS manual, to display the advisory warning message "TEST TEST Warning Message TEST TEST". The evaluator will then log out and confirm that the advisory message is displayed before logging in can occur.
Test Flow	• Create a plain text (.txt) or rich text (.rtf) document that contains the message "TEST TEST Warning Message TEST TEST". • Save the file and enter PolicyBanner for the document name. • Copy the PolicyBanner file to the /Library/Security/ folder on the TOE. • Restart the TOE so that the policy banner will take effect. • Verify that the TOE displays the advisory message "TEST TEST Warning Message TEST TEST" before logging in to the TOE again.
Pass/Fail Explanation	Pass. The TOE allows to set a login banner and successfully displays an advisory warning/login banner regarding unauthorized use of the TOE prior to establishing a user session.

Result	Pass.

6.7

6.8 Test Cases (Trusted Path/Channels)

6.8.1 FTP_ITC_EXT.1.1 Test 1

Item	Data/Description
Test ID	FTP_ITC_EXT.1.1_T1
Objective	The evaluator will configure the OS to communicate with another trusted IT product as identified in the second selection. The evaluator will monitor network traffic while the OS performs communication with each of the servers identified in the second selection. The evaluator will ensure that for each session a trusted channel was established in conformance with the protocols identified in the first selection.
Pass/Fail Explanation	Pass. This test is completed in conjunction with FCS_TLSC_EXT.1. The evaluator monitored the network traffic while the TOE established a successful connection with the TLS webserver and verified that the TOE established a trusted channel with the TLS webserver in accordance with FCS_TLSC_EXT.1.
Result	Pass.

6.8.2 FTP_TRP.1 TSS 1

The evaluator will examine the TSS to determine that the methods of remote OS administration are indicated, along with how those communications are protected. The evaluator will also confirm that all protocols listed in the TSS in support of OS administration are consistent with those specified in the requirement, and are included in the requirements in the ST.	
Evaluator Findings	The evaluator examined the TSS to determine that the methods of remote OS administration are indicated, along with how those communications are protected. The evaluator also confirmed that all protocols listed in the TSS in support of OS administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The FTP_TRP.1 entry in TSS under section 7 titled 'TOE Summary Specification' was used to determine the verdict of this activity. As per the TSS, "TOE The TOE provides a trusted path between itself and local users only using TLS v 1.2 protocol. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.3 FTP_TRP.1 Guidance 1

The evaluator will confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.	
Evaluator Findings	Tests for FTP_TRP.1.3 are not applicable because the TOE does not support remote administration methods. NIAP has approved this decision.

Verdict	Pass

6.8.4 FTP_TRP.1 Test 1

Item	Data/Description
Test ID	FTP_TRP.1_T1
Objective	The evaluator will ensure that communications using each remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
Pass/Fail Explanation	Tests for FTP_TRP.1.3 are not applicable because the TOE does not support remote administration methods. NIAP has approved this decision.

6.8.5 FTP_TRP.1 Test 2

Item	Data/Description
Test ID	FTP_TRP.1_T2
Objective	For each method of remote administration supported, the evaluator will follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.
Pass/Fail Explanation	Tests for FTP_TRP.1.3 are not applicable because the TOE does not support remote administration methods. NIAP has approved this decision.

6.8.6 FTP_TRP.1 Test 3

Item	Data/Description
Test ID	FTP_TRP.1_T3
Objective	The evaluator will ensure, for each method of remote administration, the channel data is not sent in plaintext.
Pass/Fail Explanation	Tests for FTP_TRP.1.3 are not applicable because the TOE does not support remote administration methods. Testing is not applicable. NIAP has approved this decision.

6.8.7 FTP_TRP.1 Test 4

Item	Data/Description
Test ID	FTP_TRP.1_T4
Objective	The evaluator will ensure, for each method of remote administration, modification of the channel data is detected by the OS.

Pass/Fail Explanation	Tests for FTP_TRP.1.3 are not applicable because the TOE does not support remote administration methods. Testing is not applicable. NIAP has approved this decision.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Development

There are no specific evaluation activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1 Security Functional Requirements, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.	
Evaluator Findings	As per this PP, the Evaluation Activities for this family focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional 'functional specification' documentation is necessary to satisfy the Evaluation Activities specified in the ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

Some of the contents of the operational guidance are verified by the evaluation activities in Section 5.1 Security Functional Requirements, and evaluation of the OS according to the [CEM]. The following additional information is also required. If cryptographic functions are provided by the OS, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the OS. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the OS. The documentation must describe the process for verifying updates to the OS by verifying a digital signature – this may be done by the OS or the underlying platform. The evaluator will verify that this process includes the following steps: Instructions for obtaining the update itself. This should include instructions for making the update accessible to the OS (e.g., placement in a specific directory). **Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature. The OS will likely contain security functionality that does not fall in the scope of evaluation under this PP. The**

operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.	
Evaluator Findings	The evaluator examined the Guidance document to verify that it contains guidance on performing various operations on the TOE. The evaluator found that Section 4 “Installation of the Apple macOS Catalina 10.15” provides instructions for configuring the TOE for proper operation. Section 6 “Installing Updates” provides instructions to the Administrator for performing both OS updates and Software Application updates. Step by step instructions are provided for the administrator to follow, including downloading the image, copying it to the TOE and installing it. Section 9 “TOE Cryptographic Operation – Hashing, Encryption and Decryption” of the AGD describes guidelines for configuring hashing, encryption and decryption operations on the TOE. The entirety of the Guidance documentation identifies the evaluated capabilities of the TOE by describing how to configure each functionality.
Verdict	Pass.

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1 Guidance 1

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the OS adequately addresses all platforms claimed for the OS in the ST.	
Evaluator Findings	The evaluator used the guidance documentation when configuring the TOE. The completeness of the documentation is addressed by its use in the Assurance Activities carried out in the evaluation.
Verdict	Pass.

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1 TSS 1

The evaluator will check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator will check the AGD guidance and OS samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the OS, the evaluator will examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same versions and software. The information is specific enough to procure the TOE and it includes software versions. The evaluator checked the TOE software version during testing by examining the actual machines used for testing.
Verdict	Pass.

7.4.2 ALC_CMS.1 Guidance 1

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the OS is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation. **The evaluator will ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler and linker flags). The evaluator will ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator will ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.**	
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same product versions and software. The information is specific enough to procure the TOE and it includes software versions. The evaluator checked the TOE software version during testing by examining the actual machines used for testing. The section 10 "Buffer Overflow Protections" of AGD provides instructions to create programs that have buffer overflow and ASLR protections enabled. The AGD states that "The TOE employs Stack-based Buffer Overflow Protections (SBOP) using address space layout randomization and non-executable stack and heap. The host platforms of the TOE support a feature called the NX bit which allows the operating system to mark certain parts of memory as non-executable. If the

	processor tries to execute code in any memory page marked as non-executable, the program will crash. The TOE leverages this feature by marking the stack and heap as non-executable. This makes buffer overflow attacks difficult because any attack(s) that places executable code on the stack or heap and then tries to execute that code will fail". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1 Test 1

The evaluator will prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP's evaluation activities.

While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform.

This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results.

The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and

then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.	
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.
Verdict	Pass.

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1 Test #1

The evaluator will generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. The evaluator documents the sources consulted and the vulnerabilities found in the report. **For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.**	
Evaluator Findings	The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The sources of the publicly available information are provided below. The evaluator searched the Internet for potential vulnerabilities in the TOE on June 11, 2020, August 18, 2020 and September 16, 2020. The National Vulnerability Database (NVD) was searched for publicly reported CVEs.

	The evaluator performed the public domain vulnerability searches on the following components of the TOE: • 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 • TLS1.2 The search returned no exploitable remote vulnerabilities. The residual vulnerabilities were determined not to be applicable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

8 Technical Decisions

The following Technical Decisions apply to the GPOSPP v4.2.1 Identifier	**Applicable**	**Exclusion Rationale (if applicable)**
TD0525: Updates to Certificate Revocation (FIA_X509_EXT.1)	Yes	
TD0496: GPOS PP adds allow-with statement for VPN Client V2.1	Yes	
TD0493: X.509v3 certificates when using digital signatures for Boot Integrity	Yes	
TD0463 - Clarification for FPT_TUD_EXT	Yes	
TD0441 - Updated TLS Ciphersuites for OS PP	No	The following ciphersuites are not being claimed: FCS_TLSC_EXT.1.1 in the OS PP omits the TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, and TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ciphersuites.
TD0386 – Platform-Provided Verification of Update	Yes	
TD0365 – FCS_CKM_EXT.4 selections	Yes	

Table 6 GPOS Technical Decisions

9 Conclusion

All test cases and Assurance Activities required for conformance have passed.

End of Document