Assurance Activity Report for
Apple FileVault 2 on T2 systems running macOS Catalina 10.15

Apple FileVault 2 on T2 systems running macOS Catalina 10.15 Security Target
Version 2.5

collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0e
collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0e

AAR Version 1.9, April 2021

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:

Danielle Canoles

Rutwij Kulkarni

Dayanandini Pathmanathan

Acumen Security, LLC.

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	November 2020	Initial Release
1.1	December 2020	Update based on updated ST
1.2	January 2021	Internal Review
1.3	February 2021	Updates based on updated ST and AGD
1.4	March 2021	Internal Review
1.5	March 2021	Updates based on updated vendor documents
1.6	March 2021	Updates based on updated ST
1.7	April 2021	Updates based on validator feedback
1.8	April 2021	Updates bases on validator feedback
1.9	April 2021	Updates bases on validator feedback

Contents

1 TOE Overview

The TOE is a full drive encryption product which supports both authorization acquisition and the encryption engine. The TOE is Unix-based Operating System (OS) which leverages the Apple T2 security chip (T2 security chip) to perform the full disk encryption. The OS core is a POSIX compliant OS built on top of the XNU kernel with standard Unix facilities available from the command line interface.

1.1 TOE Description

1.1.1 Evaluated Configuration

The TOE is comprised of both software and hardware. The TOE hardware consists of the Apple T2 Security Chip which is a custom silicon for the Mac. It contains the Secure Enclave coprocessor which provides security related functionality for all the EE functionality (i.e., other than encryption/decryption of storage data) and all of the cryptographic functionality for AA (i.e., PBKDF2). The Password Acquisition component (AA) is the pre-boot component on the disk and captures the user password and passes it to the T2/SEP. The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the storage and main memory of the host platform. The T2 chip is placed in the data path between the Intel chip and the storage, enabling it to encrypt/decrypt all data flowing between these two components.

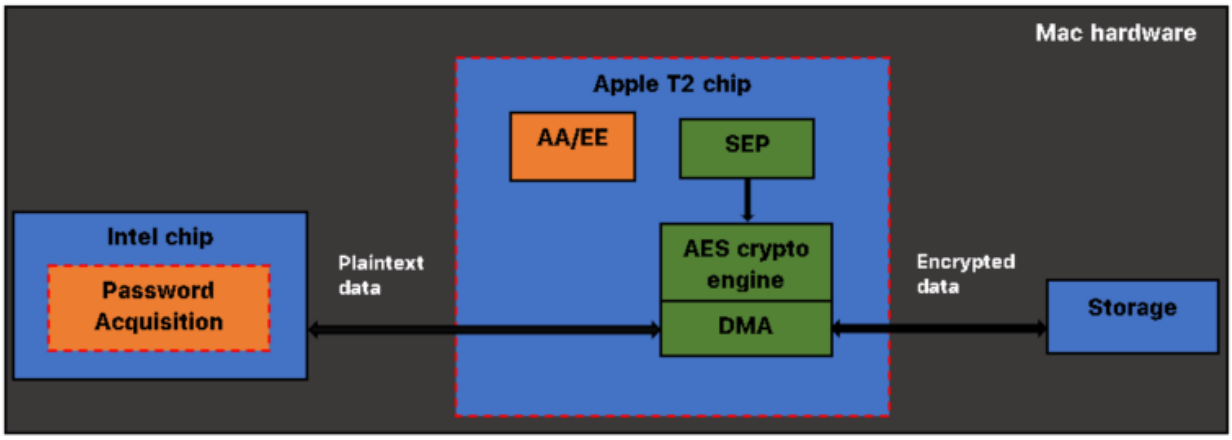

Figure 1: Major components of TOE within red border

The TOE also supports secure connectivity with an Apple update server as described in Table 1 below:

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

Table 1: IT Environment Components

Table 2 below provides a list of supported platforms:

Device	Year	Intel Processor	Apple T2 Chip
iMac Pro Model: A1862 Reference: iMac Pro1,1	Late 2017	Intel Xeon W-2140B (Skylake)	Apple T2 (ARM64) Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15
iMac Pro Model: A1862 Reference: iMac Pro1,1	Late 2017	Intel Xeon W-2150B (Skylake)	
iMac Pro Model: A1862 Reference: iMac Pro1,1	Late 2017	Intel Xeon W-2170B (Skylake)	
iMac Pro Model: A1862 Reference: iMac Pro1,1	Late 2017	Intel Xeon W-2191B (Skylake)	
Mac mini Model: A1993 Reference: Macmini8,1	2018	Intel Core i5-8500B (Coffee Lake)	
Mac mini Model: A1993 Reference: Macmini8,1	2018	Intel Core i7-8700B (Coffee Lake)	
MacBook Pro Model: A1989 Reference: MacBookPro15,2	Mid 2018	Intel Core i5-8279U (Coffee Lake)	
MacBook Pro Model: 1989 Reference: MacBookPro15,2	Mid 2018	Intel Core i5-8259U (Coffee Lake)	
MacBook Pro Model: A1990 Reference: MacBookPro15,1	Mid 2018	Intel Core i7-8750H (Coffee Lake)	
MacBook Pro Model: A1989 Reference: MacBookPro15,2	Mid 2018	Intel Core i7-8559U (Coffee Lake)	
MacBook Pro Model: A1990 Reference: MacBookPro15,3	Mid 2018	Intel Core i7-8850H (Coffee Lake)	

Device	Year	Intel Processor	Apple T2 Chip
MacBook Pro Model: A1990 Reference: MacBookPro15,1	Mid 2018	Intel Core i9-8950HK (Coffee Lake)	Apple T2 (ARM64) Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15
MacBook Pro Model: A1990 Reference: MacBookPro15,3	Mid 2018	Intel Core i9-8950HK (Coffee Lake)	
MacBook Air Model: A1932 Reference: MacBookAir8,1	Late 2018	Intel Core i5-8210Y (Amber Lake)	
MacBook Air Model: A1932 Reference: MacBookAir8,2	2019	Intel Core i5-8210Y (Amber Lake)	
Mac Pro Model: A1991 Reference: Mac Pro7,1	2019	Intel Xeon W-3223 (Cascade Lake)	
Mac Pro Model: A1991 Reference: Mac Pro7,1	2019	Intel Xeon W-3235 (Cascade Lake)	
Mac Pro Model: A1991 Reference: Mac Pro7,1	2019	Intel Xeon W-3245 (Cascade Lake)	
Mac Pro Model: A1991 Reference: Mac Pro7,1	2019	Intel Xeon W-3265M (Cascade Lake)	
Mac Pro Model: A1991 Reference: Mac Pro7,1	2019	Intel Xeon W-3275M (Amber Lake)	
MacBook Pro Model: A1989 Reference: MacBookPro15,2	2019	Intel Core i5-8279U (Amber Lake)	
MacBook Pro Model: A2159 Reference: MacBookPro15,4	2019	Intel Core i5-8257U (Amber Lake)	

Device	Year	Intel Processor	Apple T2 Chip
MacBook Pro Model: A1990 Reference: MacBookPro15,1	2019	Intel Core i7-9750H (Coffee Lake)	
MacBook Pro Model: A1989 Reference: MacBookPro15,2	2019	Intel Core i7-8569U (Coffee Lake)	
MacBook Pro Model: A2159 Reference: MacBookPro15,4	2019	Intel Core i7-8557U (Coffee Lake)	Apple T2 (ARM64) Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15
MacBook Pro: Model: A2141 Reference: MacBookPro16,1	2019	Intel Core i7-9750H (Coffee Lake)	
MacBook Pro Model: A1990 Reference: MacBookPro15,1	2019	Intel Core i9-9880H (Coffee Lake)	
MacBook Pro Model: A1990 Reference: MacBookPro15,1	2019	Intel Core i9-9980HK (Coffee Lake)	
MacBook Pro Model: A1990 Reference: MacBookPro15,3	2019	Intel Core i9-9880H (Coffee Lake)	
MacBook Pro Model: A2141 Reference: MacBookPro16,1	2019	Intel Core i9-9880H (Coffee Lake)	Apple T2(ARM 64) Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15
MacBook Pro Model: A2141 Reference: MacBookPro16,1	2019	Intel Core i9-9980HK (Coffee Lake)	
MacBook Pro Model: A2141 Reference: MacBook Pro16,4	2019	Intel Core i7-9750H (Coffee Lake)	
MacBook Pro Model: A2141 Reference: MacBook Pro16,4	2019	Intel Core i9-9880H (Coffee Lake)	

Device	Year	Intel Processor	Apple T2 Chip
MacBook Pro Model: A2141 Reference: MacBook Pro16,4	2019	Intel Core i9-9980HK (Coffee Lake)	
iMac Model: A2115 Reference: iMac20,1	2019	Intel Core i5-10500 (Ice Lake)	
Mac Pro (rack) Model: A2304 Reference: MacPro7,1	2019	Intel Xeon W-3275M (Cascade Lake)	
Mac Pro (rack) Model: A2304 Reference: MacPro7,1	2019	Intel Xeon W-3265M (Cascade Lake)	
Mac Pro (rack) Model: A2304 Reference: MacPro7,1	2019	Intel Xeon W-3245 (Cascade Lake)	
Mac Pro (rack) Model: A2304 Reference: MacPro7,1	2019	Intel Xeon W-3235 (Cascade Lake)	
Mac Pro (rack) Model: A2304 Reference: MacPro7,1	2019	Intel Xeon W-3223 (Cascade Lake)	Apple T2(ARM 64) Processor T2 (processor family arm64) from Apple family: arm64 manufacturer: Apple series: T Series Software: TxFW 10.15
MacBook Air Model: A2179 Reference: MacBook Air9,1	2020	Intel Core i5-1030NG7 (Ice Lake)	
MacBook Air Model: A2179 Reference: MacBook Air9,1	2020	Intel Core i7-1060NG7 (Ice Lake)	
MacBook Pro Model: A2289 Reference: MacBook Pro16,3	2020	Intel Core i5-8257U (Coffee Lake)	
MacBook Pro Model: A2289 Reference: MacBook Pro16,3	2020	Intel Core i7-8557U (Coffee Lake)	

Device	Year	Intel Processor	Apple T2 Chip
MacBook Pro Model: A2251 Reference: MacBook Pro16,2	2020	Intel Core i5-1037NG7 (Ice Lake)	
MacBook Pro Model: A2251 Reference: MacBook Pro16,2	2020	Intel Core i7-1068NG7 (Ice Lake)	
iMac Model: A2115 Reference: iMac20,1	2020	Intel Core i5-10600 (Ice Lake)	
iMac Model: A2115 Reference: iMac20,1	2020	Intel Core i7-10700K (Ice Lake)	
iMac Model: A2115 Reference: iMac20,1	2020	Intel Core i9-10910 (Coffee Lake)	
iMac Model: A2115 Reference: iMac20,2	2020	Intel Core i7-10700K (Ice Lake)	
iMac Model: A2115 Reference: iMac20,2	2020	Intel Core i9-10910 (Coffee Lake)	

Table 2: Platform specifications

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

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the FDEcPPs based upon the core SFRs and those implemented based on selections within the PPs.

3 Test Equivalency Justification

3.1 Introduction

This document provides a testing equivalency analysis for the Apple FileVault 2 on T2 systems running macOS Catalina 10.15.7. 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.

3.2 Architectural Description

The TOE is a full drive encryption product which supports authorization acquisition and encryption engine. The TOE 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.

3.3 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 platforms have Apple macOS Catalina v10.15.7 installed on them.

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
Amber Lake	8	i5-8210Y	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Air	MacBookAir8,2	A1932	2019	i5-8210Y	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0,
Amber Lake	8	i5-8210Y	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Air	MacBookAir8,1	A1932	Late 2018	i5-8210Y	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
Coffee Lake	8	i5-8257U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,4	A2159	2019 13-inch (Touch Bar, 2TB 3)	i5-8257U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i5-8257U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBook Pro16,3	A2289	2020, 13-inch	i5-8257U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i5-8259U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)	i5-8259U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i5-8279U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,2	A1989	2019, 13-inch (Touch Bar)	i5-8279U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i5-8279U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)	i5-8279U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW
Coffee Lake	8	i5-8500B	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	Mac mini	Macmini8,1	A1993	2018	i5-8500B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8557U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBook Pro16,3	A2289	2020, 13-inch	i7-8557U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8557U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,4	A2159	2019 13-inch (Touch Bar,	i7-8557U	• Intel® AES New Instructions, • Apple Secure Key

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
							2TB 3)		Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8559U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,2	A1989	Mid 2018, 13-inch (Touch Bar)	i7-8559U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8569U	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,2	A1989	2019, 13-inch (Touch Bar)	i7-8569U	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8700B	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	Mac mini	Macmini8,1	A1993	2018	i7-8700B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	i7-8750H	Intel® SSE4.1,	MacBook Pro	MacBookPro15,1	A1990	Mid 2018,	i7-8750H	• Intel® AES New

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
			Intel® SSE4.2, Intel® AVX2				15-inch (Touch Bar)		Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	8	I7-8850H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBook Pro15,1	A1990	Mid 2018, 15-inch (Touch Bar)	I7-8850H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i7-9750H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)	i7-9750H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i7-9750H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro16,1	A2141	2019, 16-inch	i7-9750H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									v2.0
Coffee Lake	9	i9-8950HK	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,1	A1990	Mid 2018, 15-inch (Touch Bar)	i9-8950HK	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-8950HK	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,3	A1990	Mid 2018, 15-inch (Touch Bar)	i9-8950HK	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9880H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)	i9-9880H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9880H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,3	A1990	2019, 15-inch (Touch Bar)	i9-9880H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptograph

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									ic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9880H	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro16,1	A2141	2019, 16-inch	i9-9880H	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9980HK	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,1	A1990	2019, 15-inch (Touch Bar)	i9-9980HK	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9980HK	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	MacBook Pro	MacBookPro15,3	A1990	2019, 15-inch (Touch Bar)	i9-9980HK	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Coffee Lake	9	i9-9980HK	Intel® SSE4.1, Intel® SSE4.2,	MacBook Pro	MacBookPro16,1	A2141	2019, 16-inch	i9-9980HK	• Intel® AES New Instructions,

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
			Intel® AVX2						• Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Ice lake	10	i5-1030NG7	AVX-512 Not Used by corecrypto	MacBook Air	MacBookAir9,1	A2179	2020, 13-inch scissor	i5-1030NG7	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Ice Lake	10	i5-1038NG7	AVX-512 Not Used by corecrypto	MacBook Pro	MacBook Pro16,2	A2251	2020, 13-inch	i5-1038NG7	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Ice Lake	10	i7-1068NG7	AVX-512 Not Used by corecrypto	MacBook Pro	MacBook Pro16,2	A2251	2020, 13-inch	i7-1068NG7	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
Ice Lake	10	i7-1060NG7	AVX-512 Not Used by corecrypto	MacBook Air	MacBookAir9,1	A2179	2020, 13-inch scissor	i7-1060NG7	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Skylake		W-2140B	AVX-512 Not Used by corecrypto	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017	W-2140B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Skylake		W-2150B	AVX-512 Not Used by corecrypto	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017	W-2150B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Skylake		W-2170B	AVX-512 Not Used by corecrypto	**iMac Pro**	iMacPro1,1	A1862	iMac Pro, Late 2017	W-2170B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									v10.0, • T2 SEP HW v2.0
Skylake		W-2191B	AVX-512 Not Used by corecrypto	iMac Pro	iMacPro1,1	A1862	iMac Pro, Late 2017	W-2191B	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3223	AVX-512 Not Used by corecrypto	Mac Pro	MacPro7,1	A1991	2019	W-3223	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3223	AVX-512 Not Used by corecrypto	Mac Pro(rack)	MacPro7,1	A2304	2019	W-3223	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3235	AVX-512 Not Used by corecrypto	Mac Pro	MacPro7,1	A1991	2019	W-3235	• Intel® AES New Instructions, • Apple

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3235	AVX-512 Not Used by corecrypto	Mac Pro(rack)	MacPro7,1	A2304	2019	W-3235	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3245	AVX-512 Not Used by corecrypto	Mac Pro	MacPro7,1	A1991	2019	W-3245	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3245	AVX-512 Not Used by corecrypto	Mac Pro(rack)	MacPro7,1	A2304	2019	W-3245	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
Cascade Lake		W-3265M	AVX-512 Not Used by corecrypto	Mac Pro	MacPro7,1	A1991	2019	W-3265M	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3265M	AVX-512 Not Used by corecrypto	Mac Pro(rack)	MacPro7,1	A2304	2019	W-3265M	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3275M	AVX-512 Not Used by corecrypto	Mac Pro	MacPro7,1	A1991	2019	W-3275M	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module v10.0, • T2 SEP HW v2.0
Cascade Lake		W-3275M	AVX-512 Not Used by corecrypto	Mac Pro(rack)	MacPro7,1	A2304	2019	W-3275M	• Intel® AES New Instructions, • Apple Secure Key Store Cryptographic Module

Micro-architecture	Generation	Processor-Intel Core	Instructions Set	Device Family	Hardware Reference	Model	Marketing Release Name	Documentation Links to Processor Specs	Crypto Extensions/ Accelerators
									v10.0, • T2 SEP HW v2.0

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, models A1862 and A1991 use Skylake processors and models A2115 use Comet Lake.
2. The differences between Skylake, Amber Lake, Coffee Lake, Cascade Lake and Comet 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.
4. All processing for Cryptography related to FileVault (FDE) is all performed using the Apple T2 / SEP rather than the Intel chipset, so multiple Intel Chips or microarchitectures plays no role in the processing (encryption/decryption) and the management of those keys for data under FileVault.
5. 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. 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
    c. 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

d. SSE_GFNI - SSE-based Galois Field New Instructions

e. AVX_GFNI - AVX-based Galois Field New Instructions

f. Split Lock Detection - detection and cause an exception for split locks

g. Fast Short REP MOV

6. The OS is identical on each of the platforms, and there are no differences in the crypto libraries on the platform themselves.
7. The Apple T2 chip is the same exact chip in all platforms.

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 FDE EE v2.0e + FDE AA v2.0e.

Apple T2 Security Chip and remote resting rationale is provided below:

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

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

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

3.4 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.

3.5 TOE Device Driver Differences

All device drivers in the TOE software are identical because the OS and its binaries are identical on each of the tested platforms, there are no differences in the device drivers on the platforms themselves.

3.6 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 10.15.7.

3.7 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.

3.8 Differences in Libraries Used to Provide 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.

3.9 TOE Functional Differences

The TOE boundary on each hardware model provides identical functionality. Each device runs the same version of software.

3.10 TOE Management Interfaces Differences

The user interaction with the TOE is equivalent across all the platforms; the TOE provides a login window before the user can be granted access to the TOE platform. The TOE provides the same management functions to the user across all the platforms. There are no differences between the TOE Management Interfaces across the models.

3.11 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 10.15.7
A2179	Intel Core i7-1060NG7 (Ice Lake i7)	macOS Catalina 10.15.7

Note 1: The CCTL performed the testing on Intel Core i5-8500B Coffee Lake and Intel Core i7-1060NG7 Ice Lake except for the following eight (8) SFRs.

For the following eight (8) SFRs, the vendor conducted the testing on an Intel Core i7 8557U Coffee Lake and the same test evidence was used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach was accepted by NIAP Validators during the synch meeting on 02/19/2021.

Models	Processors	Operating System
A2159	Intel Core i7-8557U (Coffee Lake i7)	macOS Catalina 10.15.7

- FCS_CKM.4(b) Test#1 [EE]

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

4 Test Bed Descriptions

4.1 Test Bed (Coffee Lake)

4.1.1 Visual Diagram #1

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

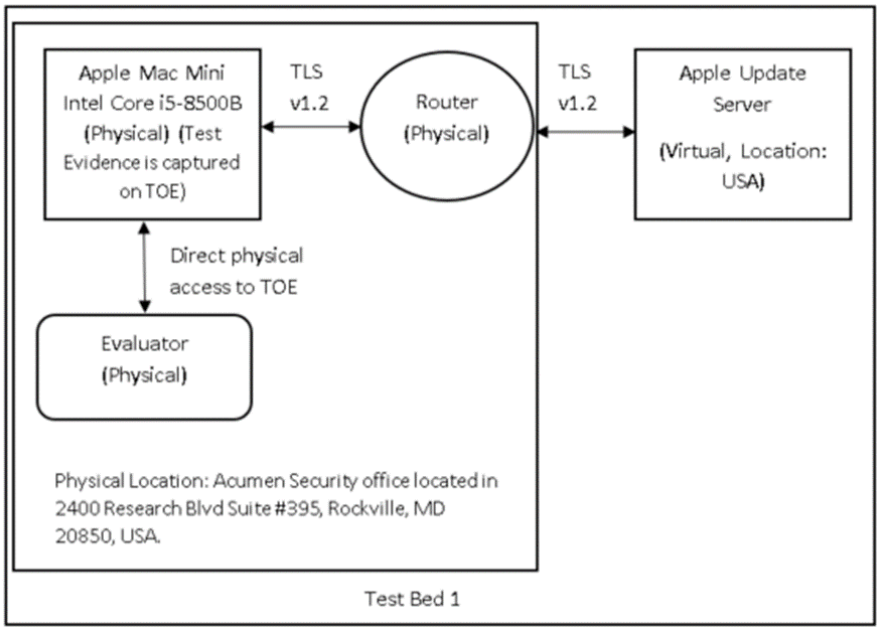

Fig 1: Test Bed 1

4.1.2 Configuration Information #1

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

Sr. No	Name	OS	Version	Function	Protocols	IP address	Tools (version)	Physical Location	Physical/Virtual Element
1	Apple Mac Mini Intel Core i5-8500B	Apple macOS Catalina	10.15.7	TOE	TLSv1.2	192.168.128.104	Disk Utility v19.0, Safari v14.0.	Acumen Security office located in 2400 Research Blvd Suite #395, Rockville, MD 20850, USA.	Physical
2	Cisco Meraki	N/A	N/A	Router	N/A	192.168.128.1	N/A		
3	Evaluator	N/A	N/A	Test the TOE and gather test evidence on the TOE.	N/A	N/A	N/A		
4	Apple Updat	N/A	N/A	Live update server	TLSv1.2	23.202.149.132	N/A	USA	The Apple Update Server is a live, virtual

Sr. No	Name	OS	Version	Function	Protocols	IP address	Tools (version)	Physical Location	Physical/Virtual Element
	e Server			that hosts TOE updates.					update server provided by Akamai. Akamai can have multiple instantiations depending on availability within the US.
Time was manually set and verified on all above identified devices. The Test Evidence was captured on the TOE.									

4.1.3 Visual Diagram #2

The diagram and configuration information below is applicable only to the following eight (8) SFRs:

- FCS_CKM.4(b) Test#1 [EE],
- FCS_CKM.4(b) Test#2 [EE],
- FCS_CKM.4(b) Test#3 [EE],
- FCS_CKM.4(d) Test#1 [AA+EE],
- FCS_CKM.4(d) Test#2 [AA+EE],
- FCS_CKM.4(d) Test#3 [AA+EE],
- FCS_VAL_EXT.1 and
- FPT_PWR_EXT.1

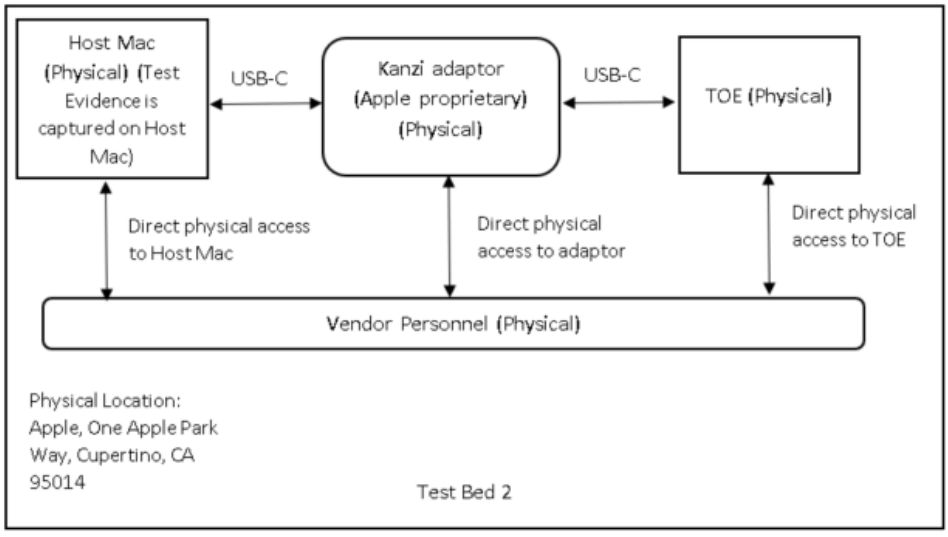

Fig 2: Test Bed 2

4.1.4 Configuration Information #2

The following table provides configuration information about each device in the test environment:

Sr. No	Name	OS	Version	Function	Protocols	IP address	Tools (version)	Physical Location	Physical/Virtual Element
1	Apple MacBook Pro 15”	Apple macOS Catalina	10.15.7	Host Mac/Vendor Personnel machine.	N/A	N/A	apfsctl crypto, diskutil, seputil ksm,key storectl.	Apple, One Apple Parkway, Cupertino, CA 95014, USA	Physical
2	Apple MacBook Pro 15 “, Intel Core i7 Coffee Lake	Apple macOS Catalina	10.15.7 debug build/Dev fused with an Apple T2 chip	TOE	N/A	N/A	N/A		
3	Kanzi Adaptor/Cable (Apple developed and proprietary)	N/A	N/A	Adaptor	N/A	N/A	N/A		
4	Vendor Personnel	N/A	N/A	Test the TOE and gather test evidence on the Host Mac.	N/A	N/A	N/A		
Time was manually set and verified on all above identified devices except Kanzi adaptor. The Test Evidence was captured on the Host Mac.									

4.3 Test Bed (Ice Lake)

4.3.1 Visual Diagram #1

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

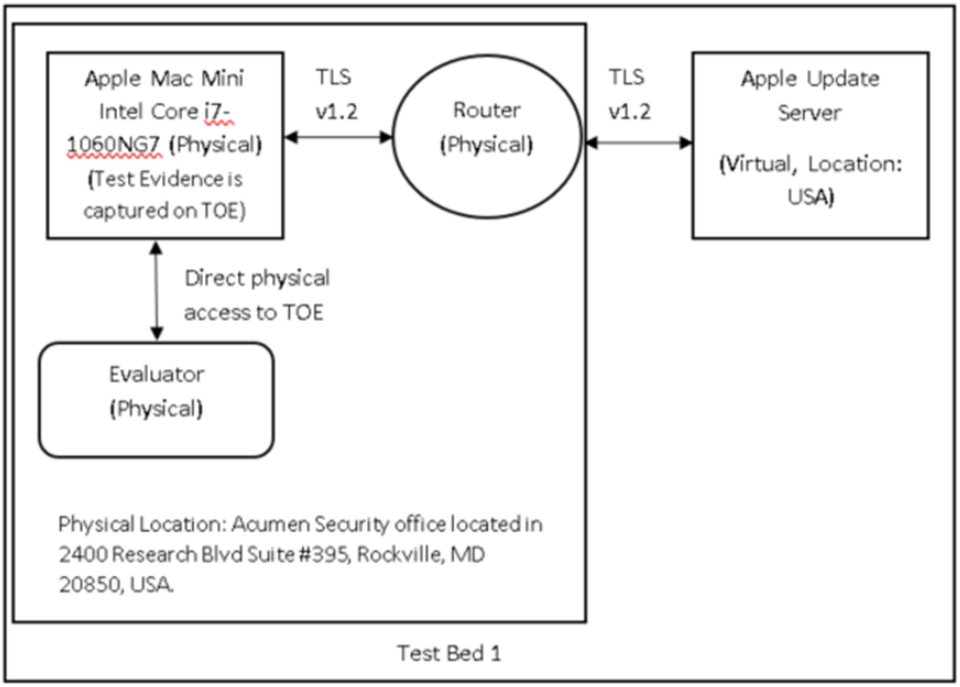

Fig 1: Test Bed 1

4.3.2 Configuration Information #1

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

Sr. No	Name	OS	Version	Function	Protocols	IP address	Tools (version)	Physical Location	Physical/Virtual Element
1	Apple Mac Mini Intel Core i7-1060NG7	Apple macOS Catalina	10.15.7	TOE	TLSv1.2	192.168.128.153	Disk Utility v19.0, Safari v14.0.	Acumen Security office located in 2400 Research Blvd Suite #395, Rockville, MD 20850, USA.	Physical
2	Cisco Meraki	N/A	N/A	Router	N/A	192.168.128.1	N/A		
3	Evaluator	N/A	N/A	Test the TOE and gather test evidence on TOE.	N/A	N/A	N/A		
4	Apple Update Server	N/A	N/A	Live update server that hosts TOE updates.	TLS v1.2	23.202.149.132	N/A	USA	The Apple Update Server is a live, virtual update server provided by Akamai. Akamai can have multiple

Sr. No	Name	OS	Version	Function	Protocols	IP address	Tools (version)	Physical Location	Physical/Virtual Element
									instantiations depending on availability within the US.
Time was manually set and verified on all above identified devices. The Test Evidence was captured on the TOE.									

4.3.3 Visual Diagram #2

Below is a visual representation of the components included in the test bed:
The diagram and configuration information below is applicable only to the following eight (8) SFRs:

- FCS_CKM.4(b) Test#1 [EE],
- FCS_CKM.4(b) Test#2 [EE],
- FCS_CKM.4(b) Test#3 [EE],
- FCS_CKM.4(d) Test#1 [AA+EE],
- FCS_CKM.4(d) Test#2 [AA+EE],
- FCS_CKM.4(d) Test#3 [AA+EE],
- FCS_VAL_EXT.1 and
- FPT_PWR_EXT.1

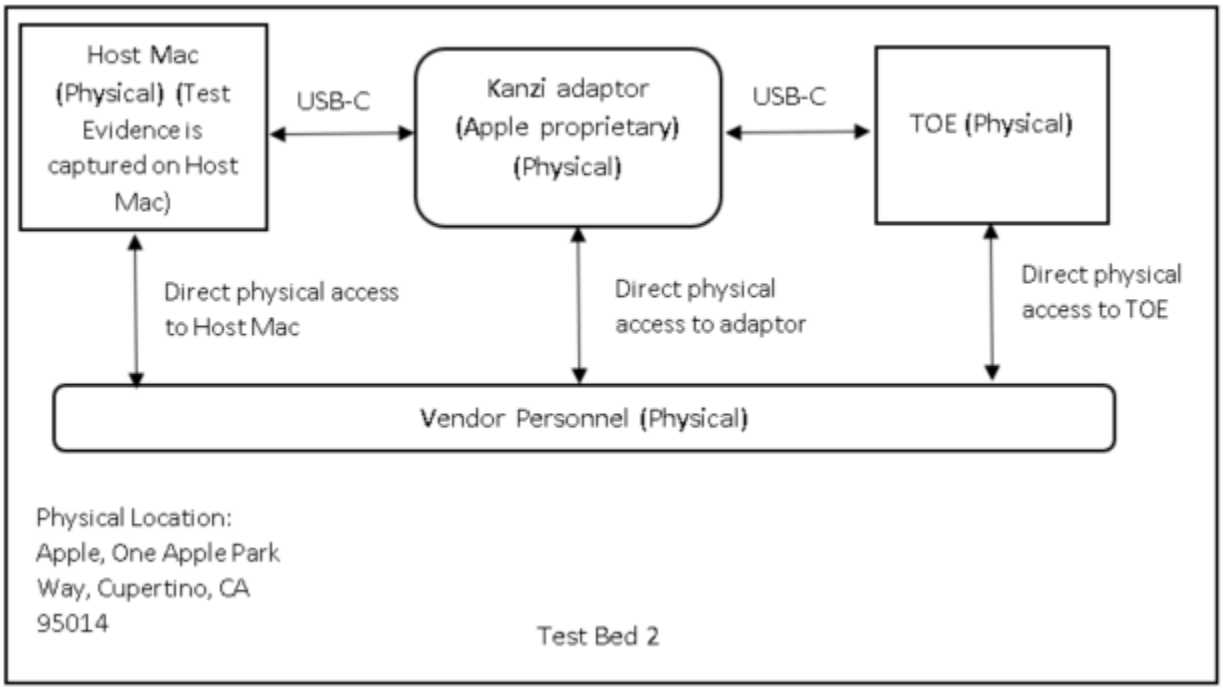

Fig 2: Test Bed 2

4.3.4 Configuration Information #2

The following table provides configuration information about each device in the test environment:

Sr. No	Name	OS	Version	Function	Protocols	MAC Address	Tools (version)	Physical Location	Physical/Virtual Element
1	Apple MacBook Pro 15”	Apple macOS Catalina	10.15.7	Host Mac/Vendor Personnel machine.	N/A	N/A	apfsctl crypto, diskutil, seputil ksm,keystorectl.	Apple, One Apple Parkway, Cupertino,	Physical

Sr. No	Name	OS	Version	Function	Protocols	MAC Address	Tools (version)	Physical Location	Physical/Virtual Element
2	Apple MacBook Pro 15 “, Intel Core i7 Coffee Lake	Apple macOS Catalina	10.15.7 debug build/Dev fused with an Apple T2 chip	TOE	N/A	N/A	N/A	CA 95014, USA.	
3	Kanzi Adaptor (Apple proprietary)	N/A	N/A	Adaptor	N/A	N/A	N/A		
4	Vendor Personnel	N/A	N/A	Test the TOE and gather test evidence on the Host Mac.	N/A	N/A	N/A		
Time was manually set and verified on all above identified devices except Kanzi adaptor. The Test Evidence was captured on the Host Mac.									

4.4 Test Time and Location

Vendor Remote Testing

For eight (8) SFRs below, the testing was performed locally by the vendor located at Apple, One Apple Park Way, Cupertino, CA 95014, on 02/18/2021 and on 02/26/2021- the CCTL witnessed this testing remotely. The testing for the SFRs below was conducted on TOE (i.e., Target Mac) and the Test evidence was captured on the Host Mac. The CCTL submitted a remote testing request to NIAP on 02/04/2021, and NIAP approved the request on 03/03/2021.

To satisfy the requirements set forth by the SFRs, the evaluation team needed access to the:

- SEP and examine the contents of the SEP.

However, due to the lack of the necessary technical means (i.e. vendor internal platform tools and techniques, debug build of the TOE, special adaptors), the evaluation team requested vendor assistance.

The physical setup for the testing is shown in the diagram below:

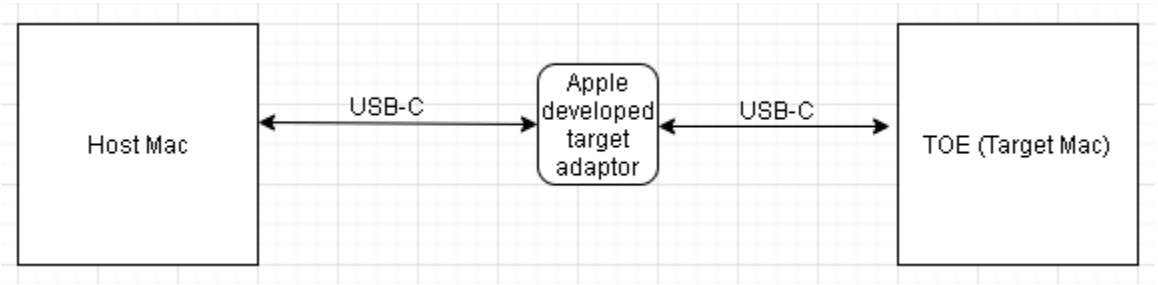

Fig 3: TOE Test bed

TOE Test bed details:

Devices:

- **TOE**: Dev-fused TOE with an Apple T2 Security Chip
- **Host Mac**: Apple internal development tools installed
- **Adaptor**: Apple developed target adaptor specific to the connector of the target machine (USB-C).

Software:

- **TOE**: Debug build of bridgeOS/sepOS Firmware loaded in TOE's T2 & SEP.
- **Host Mac**: Apple internal platform tooling with appropriate SDKs for the TOE.

Tools used in the remote testing:

- Terminal 2.11 (Terminal sessions to device- SSH (OpenSSH_8.1p1, LibreSSL 2.7.3))
- iOS menu (Menu option to SSH to device)
- iOS Toolbox v1.3.14 (Tool for access to files, executables, multi services)
- iRemoteX 1.0 (Remote control of Device via UI)

The physical access controls for the TOE included background checked employees, badge access to locked doors, security personnel (guards) for site, CCTV. The TOE and the supporting test environment were only available to authorized vendor personnel. On behalf of the vendor, only one authorized employee conducted the testing.

During the remote session, the vendor and the evaluation team constantly monitored the TOE and the supporting test bed to ensure the integrity of the TOE and the testing. In other words, the state of the test bed was not left overnight or outside of our visual. All evaluation documentation was always kept with the evaluator.

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

Evidence Integrity:

The vendor and the CCTL ensured that the remote testing session maintained its integrity throughout the entire course of the testing. The rationale below provides more details on evidence integrity.

The vendor convened and hosted a secure remote session via Cisco Webex and only authorized team members joined the remote session from their individual laptops. This remote session was further protected by an Access Code which was only shared between the vendor and the evaluation team. This ensured that only authorized personnel were permitted to join the remote session. The Webex[1] application uses HTTPS and Secure Web

[1] Cisco Webex: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf

Sockets (WSS) over TLS v1.2 for REST based signaling, and SRTP (transported over UDP/TCP/TLS) for media. This ensured the confidentiality and integrity of the data in transit.

The remote session was recorded locally by the evaluation team on their system, by using vendor owned software – Quicktime Player.

After the testing was completed, the vendor authenticated themselves to Box (i.e. Box is a third-party cloud storage solution) server via a username and password and then uploaded the test evidence to a Box folder. This Box folder was shared only with the evaluation team. Once uploaded, the evaluation team authenticated themselves to Box and then downloaded the test evidence from the Box folder. All login credentials are unique. To ensure that the test evidence maintained its integrity, the evaluation team backed up all the test evidence to Acumen systems and these systems were only accessible to authorized personnel. Prior to accessing any test evidence, the evaluation team required valid, unique login credentials to authenticate themselves to Acumen systems.

Files uploaded to Box are encrypted at rest using AES 256-bits[2]. The use of Box was mutually agreed upon between the vendor and the CCTL. The communications to and from Box servers are protected with TLS v1.2[3] thereby ensuring confidentiality and integrity for data in transit.

CCTL Testing:

Except for the eight (8) SFRs above, all the remaining testing was performed locally by Rutwij Kulkarni at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850 from 11/2019 through 02/2021.

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.

[2] Box data at rest: https://support.box.com/hc/en-us/articles/360043693854-Enhanced-Security
[3] Box data in transit: https://support.box.com/hc/en-us/articles/360043693854-Enhanced-Security

5 Detailed Test Cases (TSS, Guidance and KMD Activities)

5.1 TSS, Guidance and KMD Activities (Cryptographic Support)

5.1.1 FCS_AFA_EXT.1

5.1.1.1 FCS_AFA_EXT.1 TSS 1

Objective	The evaluator shall first examine the TSS to ensure that the authorization factors specified in the ST are described. For password-based factors the examination of the TSS section is performed as part of FCS_PCC_EXT.1 Evaluation Activities. Additionally in this case, the evaluator shall verify that the operational guidance discusses the characteristics of external authorization factors (e.g., how the authorization factor must be generated; format(s) or standards that the authorization factor must meet) that are able to be used by the TOE.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section the authorization factors specified in the ST are described. Upon investigation, the evaluator found that password-based factors are supported. Therefore, the examination of the TSS section is performed as part of FCS_PCC_EXT.1 Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 FCS_AFA_EXT.1 TSS 2

Objective	If other authorization factors [besides passwords] are specified, then for each factor, the TSS specifies how the factors are input into the TOE.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section specifies how the factors are input into the TOE. Upon investigation, the evaluator found that the TSS states: **The TOE supports password authentication factor. Passwords of up to 256 characters are supported and can be comprised of any combination of upper-case characters, lower case characters, numbers, and any other 8-bit special character.** In addition, the evaluator found that the TSS also states that for the **password-based authentication, the user's password, the TOE's UID and a salt value are used to perform a password-based derivation function (PBKDF2) and derive the Unlock Key. The UID is prefixed to the Salt value. The Unlock Key is defined as the Border Encryption Value (BEV) and is used to unwrap the Class Key with the AES Key Wrap (KW) algorithm. The password is validated if the AES KW function does not return a "Fail" result.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.4 FCS_AFA_EXT.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance includes instructions for all of the authorization factors. The AGD will discuss the characteristics of external authorization factors (e.g., how the authorization factor is generated; format(s) or standards that the authorization factor must meet, configuration of the TPM device used) that are able to be used by the TOE.
Evaluator Findings	The evaluator examined the section titled '**Authorization Factors**' in the AGD to verify that it includes instructions for all of the authorization factors and discusses the characteristics of external authorization factors that are able to be used by the TOE. Upon investigation, the evaluator found that the AGD states: **The TOE supports password as the authorization factor. Passwords of up to 256 characters are supported and can be comprised of any combination of upper-case characters, lower case characters, numbers, and any other 8-bit special character.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.5 FCS_AFA_EXT.1 KMD 1

Objective	The evaluator shall examine the Key Management Description to confirm that the initial authorization factors (submasks) directly contribute to the unwrapping of the BEV.
Evaluator Findings	The evaluator examined the sections titled '**TOE Key Hierarchy'** and **'TOE Cryptographic Keys**' in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section states that the initial authorization factors (submasks) directly contribute to the unwrapping of the BEV. Upon investigation, the evaluator found that KDM states: Unlock Key: **The Unlock Key is defined as the Border Encryption Value (BEV). It is derived from the UID and user passcode.** The submask for the Unlock key is shown in Figure 2 to be derived from the Password. Password: **This is the user password that is used to successfully unlock Full Disk Encryption (FileVault).** **To perform password-based key derivation function (PBKDF) operations, the TOE implements PBKDF2 in compliance with NIST SP 800-132. The pseudorandom function (PRF) used is HMAC-SHA-256.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.6 FCS_AFA_EXT.1 KMD 2

Objective	The evaluator shall verify the KMD describes how a submask is produced from the authorization factor (including any associated standards to which this process might conform), and verification is performed to ensure the length of the submask meets the required size (as specified in this requirement).
Evaluator Findings	The evaluator examined the section titled **'CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that these sections describe how a submask is produced from the authorization factor. Upon investigation, the evaluator found that:

	The TOE supports a password authorization factor. For password-based authentication, the user's password, the TOE's UID and a salt value are used to perform a password-based derivation function (PBKDF2) and derive the Unlock Key. The UID is prefixed to the Salt value. The Unlock Key is defined as the Border Encryption Value (BEV) and is used to unwrap the Class Key with the AES Key Wrap (KW) algorithm. The password is validated if the AES KW function does not return a "Fail" result. The Key derivation function is implemented according to NIST SP 800-132. It leverages the HMAC-SHA-256 algorithm with 50,000 iterations and the UID as the "purpose" value as defined in Appendix A.2.1 of SP 800-132. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FCS_AFA_EXT.2

5.1.2.1 FCS_AFA_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS for a description of authorization factors and which of the factors are used to gain access to user data after the TOE entered a Compliant power saving state. The TSS is inspected to ensure it describes that each authorization factor satisfies the requirements of FCS_AFA_EXT.1.1.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes authorization factors and which of the factors are used to gain access to user data after the TOE entered a Compliant power saving state. Upon investigation, the evaluator found that the TSS states: **To resume from a compliant power state, one must re-authenticate to the TOE. The user can authenticate using username and password.** The evaluator inspected the TSS ('**TOE Summary Specification**') and ensure it also describes that each authorization factor satisfies the requirements of FCS_AFA_EXT.1.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 FCS_AFA_EXT.2 Guidance 1

Objective	The evaluator shall examine the guidance documentation for a description of authorization factors used to access plaintext data when resuming from a Compliant power saving state.
Evaluator Findings	The evaluator examined the section titled '**Authorization Factors'** in the AGD to verify that it describes authorization factors used to access plaintext data when resuming from a Compliant power saving state. Upon investigation, the evaluator found that the AGD states: **The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. In order to resume from a compliant power state, the user must re-authenticate to the TOE by using a correct username and password.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FCS_CKM.1(a)

5.1.3.1 FCS_CKM.1(a) TSS 1

Objective	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 section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section identifies the key sizes supported by the TOE, and if more than one scheme is specified, it identifies the usage for each scheme. Upon investigation, the evaluator found that the TSS states: **The TOE supports RSA schemes using cryptographic key sizes of 2048-bit which meets FIPS PUB 186-4, "Digital Signature Standard (DSS)",Appendix B.3**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.2 FCS_CKM.1(a) Guidance 1

Objective	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 specified by the AGD documentation and defined in this cPP.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption**' in the AGD to verifies how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all uses specified by the AGD documentation and defined in this ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.3 FCS_CKM.1(a) Test/CAVP 1

Objective	The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Key Generation for FIPS PUB 186-4 RSA Schemes The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent e, the private prime factors p and q, the public modulus n and the calculation of the private signature exponent d. Key Pair generation specifies 5 ways (or methods) to generate the primes p and q. These include: 1. Random Primes: • Provable primes • Probable primes 2. Primes with Conditions:

	• Primes p1, p2, q1,q2, p and q shall all be provable primes • Primes p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes • Primes p1, p2, q1,q2, p and q shall all be probable primes To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Key Generation for Elliptic Curve Cryptography (ECC) FIPS 186-4 ECC Key Generation Test For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation. FIPS 186-4 Public Key Verification (PKV) Test For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values. Key Generation for Finite-Field Cryptography (FFC) The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y. The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p: Cryptographic and Field Primes: • Primes q and p shall both be provable primes • Primes q and field prime p shall both be probable primes and two ways to generate the cryptographic group generator g: Cryptographic Group Generator: • Generator g constructed through a verifiable process

	• Generator g constructed through an unverifiable process. The Key generation specifies 2 ways to generate the private key x: Private Key: • len(q) bit output of RBG where 1 <=x <= q-1 • len(q) + 64 bit output of RBG, followed by a mod (q-1) operation and +1 operation where 1<= x<=q-1. The security strength of the RBG must be at least that of the security offered by the FFC parameter set. To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set. For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm • g != 0,1 • q divides p-1 • g^q mod p = 1 • g^x mod p = y for each FFC parameter set and key pair.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: # **A495** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.4 FCS_CKM.1(a) KMD 1

Objective	If the TOE uses an asymmetric key as part of the key chain, the KMD should detail how the asymmetric key is used as part of the key chain.
Evaluator Findings	The evaluator examined the section titled '**TOE Key Hierarchy'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section details how the asymmetric key is used as part of the key chain. Upon investigation, the evaluator found that the key chain does not use any asymmetric keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.4 FCS_CKM.1(b)

5.1.4.1 FCS_CKM.1(b) TSS 1

Objective	The evaluator shall review the TSS to determine that a symmetric key is supported by the product, that the TSS includes a description of the protection provided by the product for this key. The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section states that a symmetric key is supported by the product, includes a description of the protection provided by the product for this key, and includes the key sizes supported by the TOE. Upon investigation, the evaluator found that the **TOE generates symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 with 256 bits key size.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.4.2 FCS_CKM.1(b) Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key size(s) for all uses specified by the AGD documentation and defined in this cPP.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption**' in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key size(s) for all uses specified by the AGD documentation and defined in this ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.4.3 FCS_CKM.1(b) KMD 1

Objective	If the TOE uses a symmetric key as part of the key chain, the KMD should detail how the symmetric key is used as part of the key chain.
Evaluator Findings	The evaluator examined the section titled '**TOE Key Hierarchy'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section details how the symmetric key is used as part of the key chain. Upon investigation, the evaluator found that the following usage of symmetric keys is described: • Hardware UID/Key is used with AES-CBC to process the submask derived from the Password • Unlock Key unwraps the User Keybag (which contains the Class A Key) with AES-KW • Class A Key unwraps the Volume Key, which is used to decrypt/decrypt Volume contents (DEK) Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.5 FCS_CKM.1(c)

5.1.5.1 FCS_CKM.1(c) TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes how the TOE obtains a DEK (either generating the DEK or receiving from the environment).
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE obtains a DEK (either generating the DEK or receiving from the environment). The TOE generates a DEK using the RBG as specified in FCS_RBG_EXT.1. Upon investigation, the evaluator found that the TSS describes this process stating that **all symmetric and asymmetric cryptographic keys are randomly generated internal to the TOE using the SEP's True Random Number Generator (TRNG). The SEP's TRNG is seeded by 24 ring oscillators and post processed with an SP 800-90A CTR_DRBG.** In which the evaluator found the Volume Key otherwise know as the Data Encryption Key (DEK). **It is randomly generated when a user volume is created, and the key is destroyed by issuing an authenticated command by a single overwrite consisting of zeroes.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.5.2 FCS_CKM.1(c) TSS 2

Objective	If the TOE generates a DEK, the evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked. If the DEK is generated outside of the TOE, the evaluator checks to ensure that for each platform identified in the TOE the TSS, it describes the interface used by the TOE to invoke this functionality. The evaluator uses the description of the interface between the RBG and the TOE to determine that it requests a key greater than or equal to the required key sizes.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE generates a DEK. The evaluator confirmed that this section it describes how the functionality described by FCS_RBG_EXT.1 is invoked. Upon investigation, the evaluator found that the TOE generates a DEK using the RBG as specified in FCS_RBG_EXT.1 Furthermore the evaluator found that the TSS states: **All symmetric and asymmetric cryptographic keys are randomly generated internal to the TOE using the SEP's True Random Number Generator (TRNG). The SEP's TRNG is seeded by 24 ring oscillators and post processed with an SP 800-90A CTR_DRBG. The ring oscillators are constantly inputting new noise data into the conditioner (SHA-256 hash) from which the DRBG seed is obtained. Thus, the conditioner accumulates the entropy of the ring oscillators. 0.9 bits of entropy is provided per data bit. Full entropy of 256 bits is reached after collecting 285 bits of data from the noise source. As the noise source runs faster than the DRBG, the number of data bits collected from the noise source and injected into the conditioner is always considered higher than 285 bits. Thus, the DRBG is seeded with greater than 256 bits of entropy. Key generation using the DRBG are performed by calling the DRBG's generate function.**

	The Volume Key is defined as the Data Encryption Key (DEK). It is randomly generated when a user volume is created, and the key is destroyed by issuing an authenticated command by a single overwrite consisting of zeroes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.5.3 FCS_CKM.1(c) TSS 3

Objective	If the TOE received the DEK from outside the host platform, then the evaluator shall examine the TSS to determine that the DEK is sent wrapped using the appropriate encryption algorithm.
Evaluator Findings	Upon investigation, the evaluator found that the TOE does not receive the DEK from outside the host platform. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.1.5.4 FCS_CKM.1(c) KMD 1

Objective	If the TOE received the DEK from outside the host platform, then the evaluator shall verify that the KMD describes how the TOE unwraps the DEK.
Evaluator Findings	The evaluator examined the entirety of the KMD to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TOE does not receive the DEK from outside the host platform. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.1.6 FCS_CKM.4(a)

5.1.6.1 FCS_CKM.4(a) TSS 1

Objective	The evaluator shall verify the TSS provides a high level description of how keys stored in volatile memory are destroyed. The valuator to verify that TSS outlines: - if and when the TSF or the Operational Environment is used to destroy keys from volatile memory; - if and how memory locations for (temporary) keys are tracked; - details of the interface used for key erasure when relying on the OE for memory clearing.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section provides a high level description of how keys stored in volatile memory are destroyed. Upon investigation, the evaluator found that: **The TOE leverages DRAM for volatile memory. Keys are stored in volatile memory while being used for their specific operation. Except for the UID and the Unlock Key, all symmetric keys are introduced into volatile memory after being randomly generated or by unwrapping or decrypting a key stored in non-volatile memory. The Unlock Key is introduced into volatile memory after the password-based derivation process has been completed.**

	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. Keys are only stored in volatile memory when they are required to perform a specific cryptographic operation. Since the keys are being used by the SEP to perform the operation, the SEP tracks the memory location of the key until the operation is complete. 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). **The SEP performs the encryption or wrapping of keys, which are then sent to the memory controller for storage. The memory controller takes the block of data and the memory location provided by the SEP and stores the data in memory.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.6.2 FCS_CKM.4(a) Guidance 1

Objective	The evaluator shall check the guidance documentation if the TOE depends on the Operational Environment for memory clearing and how that is achieved.
Evaluator Findings	The evaluator examined the section titled '**Key Destruction'** in the AGD to verify that it states whether TOE depends on the Operational Environment for memory clearing and how that is achieved. Upon investigation, the evaluator found that the AGD states: **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

5.1.6.3 FCS_CKM.4(a) KMD 1

Objective	The evaluator shall check to ensure the KMD lists each type of key, its origin, possible memory locations in volatile memory.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section lists each type of key, its origin, and possible memory locations in volatile memory. Upon investigation, the evaluator found that the table in this section lists each type of key, its origin, and possible memory locations in volatile memory. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7 FCS_CKM.4(b)

5.1.7.1 FCS_CKM.4(b) TSS/KMD 1

Objective	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 section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the keys are managed in volatile memory, including details of how each identified key is introduced into volatile memory and how they are overwritten. Upon investigation, the evaluator found that the table in this section states that the UID and Ephemeral Key in SEP non-volatile memory are destroyed via shutdown, while the Unlock Key, Class A Key and Volume Key in SEP non-volatile memory are destroyed via overwriting once with zeros. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7.2 FCS_CKM.4(b) TSS/KMD 2

Objective	The evaluator shall check to ensure the TSS lists each type of key that is stored, and identifies the memory type where key material is stored. When listing the type of memory employed, the TSS will list each type of memory selected in the FCS_CKM.4.1 SFR, as well as any memory types that employ a different memory controller or storage algorithm. For example, if a TOE uses NOR flash and NAND flash, both types are to be listed.
Evaluator Findings	The evaluator examined the sections titled '**TOE Cryptographic Keys'** in the KMD and '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section lists each type of key that is stored, and identifies the memory type where key material is stored. Upon investigation, the evaluator found that the section titled '**TOE Cryptographic Keys'** describes and lists each type of key that is stored and the type of memory (volatile or non-volatile) where the key material is stored. The evaluator also examined the section titled '**TOE Summary Specification**' in the Security Target which states the **TOE leverages NAND flash for non-volatile memory** and **DRAM for volatile memory.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7.3 FCS_CKM.4(b) TSS/KMD 3

Objective	The evaluator shall examine the TSS to ensure it describes the method that is used by the memory controller to write and read memory from each type of memory listed. The purpose here is to provide a description of how the memory controller works so one can determine exactly how keys are written to memory. The description would include how the data is written to and read from memory (e.g., block level, cell level), mechanisms for copies of the key that could potentially exist (e.g., a copy with parity bits, a copy without parity bits, any mechanisms that are used for redundancy).

Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification**' and '**Key Management Description'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the method that is used by the memory controller to write and read memory from each type of memory listed, including how the data is written to and read from memory. Upon investigation, the evaluator found that the TSS states: **The SEP performs the encryption or wrapping of keys, which are then sent to the memory controller for storage. The memory controller takes the block of data and the memory location provided by the SEP and stores the data in memory.** . Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7.4 FCS_CKM.4(b) TSS/KMD 4

Objective	The evaluator shall examine the TSS to ensure it describes the destruction procedure for each key that has been identified. If different types of memory are used to store the key(s), the evaluator shall check to ensure that the TSS identifies the destruction procedure for each memory type where keys are stored (e.g., key X stored in flash memory is destroyed by overwriting once with zeros, key X' stored in EEPROM is destroyed by a overwrite consisting of a pseudo random pattern – the EEPROM used in the TOE uses a wear-leveling scheme as described).
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the destruction procedure for each key that has been identified and the destruction procedure for each memory type where keys are stored. Upon investigation, the evaluator found that the table in this section describes the destruction procedure for each key, including the method used volatile (DRAM) and non-volatile (NAND) memory. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7.5 FCS_CKM.4(b) TSS/KMD 5

Objective	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 shall verify that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification**' and '**Key Management Description'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that the ST does not make use of the open assignment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.7.6 FCS_CKM.4(b) TSS/KMD 6

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification**' and '**Key Management Description'** in the Security Target to determine the verdict of this assurance

	activity. The evaluator confirmed that this section identifies any configurations or circumstances that may not strictly conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states: **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

5.1.7.7 FCS_CKM.4(b) Guidance 1

Objective	There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall 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. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled '**Key Destruction'** in the AGD to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement; that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information; and provides guidance on situations where key destruction may be delayed at the physical layer. Upon investigation, the evaluator found that the AGD states: **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

5.1.8 FCS_CKM.4(d)

5.1.8.1 FCS_CKM.4(d) TSS/KMD 1

Objective	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 section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the keys are managed in volatile memory, including details of how each identified key is introduced into volatile memory and how they are overwritten. Upon investigation, the evaluator found that the table in this section describes how each key is introduced (via

	derivation, unwrapping or decryption) and how they are overwritten once with zeros or destroyed via shutdown. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.8.2 FCS_CKM.4(d) TSS/KMD 2

Objective	The evaluator shall 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 sections titled '**Apple File System (APFS) encrypted storage'** and **'TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section 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). Upon investigation, the evaluator found that the table in **'TOE Cryptographic Keys'** lists where each key is stored and how it is stored. In addition, the evaluator found that Figure 1 in '**Apple File System (APFS) encrypted storage'** shows that the Secure Enclave Processor utilizes dedicated Secure Nonvolatile Storage. The interface to this storage is entirely within the Secure Enclave Processor. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.8.3 FCS_CKM.4(d) TSS/KMD 3

Objective	The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) and description in the TSS.
Evaluator Findings	The evaluator examined the section titled '**Apple File System (APFS) encrypted storage'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that the interface description for each different media type to ensure that the interface supports the selection(s) and description in the TSS. Upon investigation, the evaluator found that Figure 1 in the KDM in section titled '**Apple File System (APFS) encrypted storage**' includes interfaces to nonvolatile storage (NAND) and volatile storage (DRAM). These media types are consistent with the TSS and SFR selections in the Security Target. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.8.4 FCS_CKM.4(d) TSS/KMD 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement. 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 shall verify that the pattern does not contain any CSPs.
Evaluator Findings	Upon investigation, the evaluator checked section titled '**TOE Summary Specification**' and found that the TSS does identifies configurations and circumstances that may not strictly conform to the key destruction requirement. The evaluator found that for cryptographic keys that are stored in Volatile memory and/or Non-Volatile memory, the TOE destroys the cryptographic keys with a single overwrite consisting of zeroes. In addition, the TSS states: **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

5.1.8.5 FCS_CKM.4(d) Guidance 1

Objective	There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall 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. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled '**Key Destruction'** in the AGD to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement, that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information, and that the AGD provides guidance on situations where key destruction may be delayed at the physical layer. Upon investigation, the evaluator found that the AGD states: **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

5.1.9 FCS_CKM_EXT.4(a)

5.1.9.1 FCS_CKM_EXT.4(a) TSS 1

Objective	The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed. Upon investigation, the evaluator found that the TSS states: **The TOE will destroy all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1.** **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

5.1.9.2 FCS_CKM_EXT.4(a) KMD 1

Objective	The evaluator shall verify the KMD includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed. Upon investigation, the evaluator found that the table in this section includes, for each key, the area where the key resides and a description of when the keys are no longer required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.9.3 FCS_CKM_EXT.4(a) KMD 2

Objective	The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4(a) for the destruction.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the table in this section includes a key lifecycle description including where key material resides, how the key material is used, and how the material is destroyed once it is not needed (which follows the requirements for FCS_CKM.4(a) for the destruction). Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.1.10 FCS_CKM_EXT.4(b)

5.1.10.1 FCS_CKM_EXT.4(b) TSS 1

Objective	The evaluator shall verify the TSS provides a description of what keys and key material are destroyed when entering any Compliant power saving state.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section provides a description of what keys and key material are destroyed when entering any Compliant power saving state. Upon investigation, the evaluator found that the TSS states: **The TOE will destroy all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.10.2 FCS_CKM_EXT.4(b) Guidance 1

Objective	The evaluator shall validate that guidance documentation contains clear warnings and information on conditions in which the TOE may end up in a non-Compliant power saving state indistinguishable from a Compliant power saving state. In that case it must contain mitigation instructions on what to do in such scenarios.
Evaluator Findings	The evaluator examined the section titled '**Authorization Factors'** and '**Validation of Cryptographic Elements'** in the AGD to verify that it contains clear warnings and information on conditions in which the TOE may end up in a non-Compliant power saving state indistinguishable from a Compliant power saving state. Upon investigation, the evaluator found that the AGD states: **The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. In order to resume from a compliant power state, the user must re-authenticate to the TOE. The user can authenticate using username and password.** The evaluator verified that section titled '**Validation of Cryptographic Elements'** in the AGD contains mitigation instructions on what to do in such scenarios. Upon investigation, the evaluator found that the AGD states: **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.10.3 FCS_CKM_EXT.4(b) KMD 1

Objective	The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the areas where keys and key material reside. Upon investigation, the evaluator found that the table in this section describes areas where keys and key material reside. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.10.4 FCS_CKM_EXT.4(b) KMD 2

Objective	The evaluator shall verify the KMD includes a key lifecycle that includes a description where key material resides, how the key material is used, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4(d) for the destruction.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the table in this section includes a key lifecycle description where key material resides, how the key material is used, and how the material is destroyed once it is not needed (which follows the requirements for FCS_CKM.4(d) for the destruction). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.11 FCS_CKM_EXT.6

5.1.11.1 FCS_CKM_EXT.6 TSS/KMD 1

Objective	The evaluator shall examine the TOE's keychain in the TSS/KMD and verify all keys subject to destruction are destroyed according to one of the specified methods.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section states that all keys subject to destruction are destroyed according to one of the specified methods. Upon investigation, the evaluator found that the table in this section states that all keys are destroyed by overwriting once with zeros or via shutdown. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.12 FCS_COP.1(a)

5.1.12.1 FCS_COP.1(a) TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes the overall flow of the signature verification. This should at least include identification of the format and general location (e.g., "firmware on the hard drive device" rather than “memory location 0x00007A4B") of the data to be used in verifying the digital signature; how the data received from the operational environment are brought on to the device; and any processing that is performed that is not part of the digital signature algorithm (for instance, checking of certificate revocation lists).
Evaluator Findings	The evaluator examined the section titled ‘**TOE Summary Specification’** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the overall flow of the signature verification, including identification of the format and general location of the data to be used in verifying the digital signature; how the data received from the operational environment are brought on to the device; and any processing that is performed that is not part of the digital signature algorithm. Upon investigation, the evaluator found that the TSS states: **Signature verification is done as part of the Secure Boot process, for firmware and software updates. Signatures are verified using RSA 2048-bit and SHA-256. The CA Public Key is embedded in the SEP’s Boot ROM code in manufacturing and is used for all macOS running on Mac hardware with Apple T2 chip. The TOE image is signed using this key’s corresponding private key.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.12.2 FCS_COP.1(a) Test/CAVP 1

Objective	Each section below contains the tests the evaluators must perform for each type of digital signature scheme. Based on the assignments and selections in the requirement, the evaluators choose the specific activities that correspond to those selections. It should be noted that for the schemes given below, there are no key generation/domain parameter generation testing requirements. This is because it is not anticipated that this functionality would be needed in the end device, since the functionality is limited to checking digital signatures in delivered updates. This means that the domain parameters should have already been generated and encapsulated in the hard drive firmware or on-board non-volatile storage. If key generation/domain parameter generation is required, the evaluation and validation scheme must be consulted to ensure the correct specification of the required evaluation activities and any additional components. The following tests are conditional based upon the selections made within the SFR. The following tests may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. ECDSA Algorithm Tests ECDSA FIPS 186-4 Signature Verification Test For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.

	RSA Signature Algorithm Tests Signature Verification Test The evaluator shall perform the Signature Verification test to verify the ability of the TOE to recognize another party's authentic and unauthentic signatures. The evaluator shall inject errors into the test vectors produced during the Signature Verification Test by introducing errors in some of the public keys e, messages, IR format, and/or signatures. The TOE attempts to verify the signatures and returns success or failure. The evaluator shall use these test vectors to emulate the signature verification test using the corresponding parameters and verify that the TOE detects these errors.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: RSA # **A495** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.13 FCS_COP.1(b)

5.1.13.1 FCS_COP.1(b) TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that the **TOE supports SHA-256 algorithm to perform digital signature verification of 2048 bit RSA keys and in HMAC operations.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.13.2 FCS_COP.1(b) Guidance 1

Objective	The evaluator checks the operational guidance documents to determine that any system configuration necessary to enable required hash size functionality is provided.
Evaluator Findings	The evaluator checked the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption'** in the AGD to verify that configurations necessary to enable required hash size functionality is provided. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.13.3 FCS_COP.1(b) Test/CAVP 1

Objective	The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode. The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this cPP. <u>Short Messages Test Bit-oriented Mode</u> The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Short Messages Test Byte-oriented Mode</u> The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Selected Long Messages Test Bit-oriented Mode</u> The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-384 and SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Selected Long Messages Test Byte-oriented Mode</u> The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-384 and SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Pseudorandomly Generated Messages Test</u> This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of the NIST Secure Hash Algorithm Validation System (SHAVS)

	(https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-ValidationProgram/documents/shs/SHAVS.pdf). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: SHA # **A497, A495, A500** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.14 FCS_COP.1(c)

5.1.14.1 FCS_COP.1(c) TSS 1

Objective	**(conditional)** If HMAC was selected: The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that the **TOE supports keyed hash algorithm with HMAC-SHA-256 supporting key size of 256 bits and block size of 512 bits. SHA-256 hashing function is used.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.14.2 FCS_COP.1(c) Test/CAVP 1

Objective	If HMAC was selected: For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key using a known good implementation. If CMAC was selected: For each of the supported parameter sets, the evaluator shall compose at least 15 sets of test data. Each set shall consist of a key and message data. The test data shall include messages of different lengths, some with partial blocks as the last block and some with full blocks as the last block. The test data keys shall include cases for which subkey K1 is generated both with and without using the irreducible polynomial R_b, as well as cases for which subkey K2 is generated from K1 both with and without using the irreducible polynomial R_b. (The subkey generation and polynomial R_b are as defined in SP800-38E.) The evaluator shall have the TSF generate CMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating CMAC tags with the same key using a known good implementation.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: HMAC # **A497, A495, A500**

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

5.1.15 FCS_COP.1(d)

5.1.15.1 FCS_COP.1(d) TSS 1

Objective	The evaluator shall verify the TSS includes a description of the key wrap function(s) and shall verify the key wrap uses an approved key wrap algorithm according to the appropriate specification.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the key wrap function(s) and verifies the key wrap uses an approved key wrap algorithm according to the appropriate specification. Upon investigation, the evaluator found that the TSS states: **When the User requests a crypto service from the module, it must provide the passcode and a reference to the user keybag that is stored encrypted under SP800-38F AES Key Wrapping (AES-KW) within SKS. The module uses PBKDF to derive an AES key from the Operator provided passcode. The derived AES key is then used by the module's SP800-38F AES Key Unwrapping function (i.e. AES-KW-AD3) to decrypt the referenced user keybag and to verify the authenticity of the decrypted key. As AES-KW is an authentication cipher, the decryption operation will only succeed without an authentication error. This implies that the user provided the correct passcode to derive the correct AES key for AES Key Unwrapping. Any other passcode will derive a different AES key which will result in a wrong decrypted user key that fails the authentication check. If the user keybag can be successfully unwrapped, the user is authenticated to the module and the requested crypto service will then be proceeded with the unwrapped user key. The failure of unwrapping user keybag is also a user authentication failure and the Operator will be denied access to the module.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.15.2 FCS_COP.1(d) KMD 1

Objective	The evaluator shall review the KMD to ensure that all keys are wrapped using the approved method and a description of when the key wrapping occurs.
Evaluator Findings	The evaluator examined the sections titled '**TOE Cryptographic Keys'** and **'CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that all keys are wrapped using the approved method and a description of when the key wrapping occurs. Upon investigation, the evaluator found that the table in the '**TOE Cryptographic Keys'** section states "The SEP derives the Unlock Key from the UID/Password and unwraps the User Keybag which makes the Class A Key (KEK) Available to the SEP to unwrap the VEK." In addition, the evaluator found that the **'CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** section states that keys are wrapped using "SP800-38F AES Key Wrapping (AES-KW)". Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.1.16 FCS_COP.1(f)

5.1.16.1 FCS_COP.1(f) TSS 1

Objective	The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the key size used for encryption and the mode used for encryption. Upon investigation, the evaluator found that the TSS states that the **TOE supports AES data encryption and AES decryption using AES-128 in XTS mode. The key size supported is 256 bits.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.16.2 FCS_COP.1(f) Guidance 1

Objective	If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption'** in the AGD to verify that it describes the method of choosing a specific mode/key size by the end user. Upon investigation, the evaluator found that the AGD states: **The TOE supports AES data encryption and AES decryption using AES in XTS mode that meet the following: AES as specified in ISO/IEC18033-3 and XTS as specified in IEEE 1619. The key size supported is 256-bits. The TOE supports key encryption and decryption using AES algorithm as specified in ISO/IEC 18033-3. The modes supported are CBC, as specified in ISO/IEC 10116 and GCM, as specified in ISO/IEC 19772. The key size supported is 256 bits.** **Note: The TOE supports AES data encryption and AES decryption by default and no configuration is required.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.16.3 FCS_COP.1(f) Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: AES-XTS # **A494** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.17 FCS_COP.1(g)

5.1.17.1 FCS_COP.1(g) TSS 1

Objective	The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for the key encryption.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the key size used for encryption and the mode used for the key encryption. Upon investigation, the evaluator found that the **TOE supports key encryption and decryption using AES algorithm. The modes supported are CBC and GCM modes. The key size supported is 256 bits.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.17.2 FCS_COP.1(g) & (f) Test/CAVP 1

Objective	The following tests are conditional based upon the selections made in the SFR. <u>AES-CBC Tests</u> For the AES-CBC tests described below, the plaintext, ciphertext, and IV values shall consist of 128-bit blocks. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known-good implementation. These tests are intended to be equivalent to those described in NIST's AES Algorithm Validation Suite (AESAVS) (http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf). Known answer values tailored to exercise the AES-CBC implementation can be obtained using NIST's CAVS Algorithm Validation Tool or from NIST's ACPV service for automated algorithm tests (acvp.nist.gov), when available. It is not recommended that evaluators use values obtained from static sources such as the example NIST's AES Known Answer Test Values from the AESAVS document, or use values not generated expressly to exercise the AES-CBC implementation. AES-CBC Known Answer Tests KAT-1 (GFSBox): To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of five different plaintext values for each selected key size and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. To test the decrypt functionality of AES-CBC, the evaluator shall supply a set of five different ciphertext values for each selected key size and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using a key value of all zeros and an IV of all zeros. KAT-2 (KeySBox): To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of five

	different key values for each selected key size and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. To test the decrypt functionality of AES-CBC, the evaluator shall supply a set of five different key values for each selected key size and obtain the plaintext that results from AES-CBC decryption of an all-zeros ciphertext using the given key and an IV of all zeros. KAT-3 (Variable Key): To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of keys for each selected key size (as described below) and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using each key and an IV of all zeros. Key i in each set shall have the leftmost i bits set to ones and the remaining bits to zeros, for values of i from 1 to the key size. The keys and corresponding ciphertext are listed in AESAVS, Appendix E. To test the decrypt functionality of AES-CBC, the evaluator shall use the same keys as above to decrypt the ciphertext results from above. Each decryption should result in an all-zeros plaintext. KAT-4 (Variable Text): To test the encrypt functionality of AES-CBC, for each selected key size, the evaluator shall supply a set of 128-bit plaintext values (as described below) and obtain the ciphertext values that result from AES-CBC encryption of each plaintext value using a key of each size and IV consisting of all zeros. Plaintext value i shall have the leftmost i bits set to ones and the remaining bits set to zeros, for values of i from 1 to 128. The plaintext values are listed in AESAVS, Appendix D. To test the decrypt functionality of AES-CBC, for each selected key size, use the plaintext values from above as ciphertext input, and AES-CBC decrypt each ciphertext value using key of each size consisting of all zeros and an IV of all zeros. AES-CBC Multi-Block Message Test The evaluator shall test the encrypt functionality by encrypting nine i-block messages for each selected key size, for $2 \leq i \leq 10$. For each test, the evaluator shall supply a key, an IV, and a plaintext message of length i blocks, and encrypt the message using AES-CBC. The resulting ciphertext values shall be compared to the results of encrypting the plaintext messages using a known good implementation. The evaluator shall test the decrypt functionality by decrypting nine i-block messages for each selected key size, for $2 \leq i \leq 10$. For each test, the evaluator shall supply a key, an IV, and a ciphertext message of length i blocks, and decrypt the message using AESCBC. The resulting plaintext values shall be compared to the results of decrypting the ciphertext messages using a known good implementation.

AES-CBC Monte Carlo Tests

The evaluator shall test the encrypt functionality for each selected key size using 100 3-tuples of pseudo-random values for plaintext, IVs, and keys.
237 The evaluator shall supply a single 3-tuple of pseudo-random values for each selected key size. This 3-tuple of plaintext, IV, and key is provided as input to the below algorithm to generate the remaining 99 3-tuples, and to run each 3-tuple through 1000 iterations of AES-CBC encryption.

```
# Input: PT, IV, Key
Key[0] = Key
IV[0] = IV
PT[0] = PT
for i = 1 to 100 {
Output Key[i], IV[i], PT[0]for j = 1 to 1000 {
if j == 1 {
CT[1] = AES-CBC-Encrypt(Key[i], IV[i], PT[1])
PT[2] = IV[i]
} else {
CT[j] = AES-CBC-Encrypt(Key[i], PT[j])
PT[j+1] = CT[j-1]
}
 }
Output CT[1000]
If KeySize == 128 { Key[i+1] = Key[i] xor CT[1000] }
If KeySize == 256 { Key[i+1] = Key[i] xor ((CT[999] << 128) | CT[1000]) }
IV[i+1] = CT[1000]
PT[0] = CT[999]
 }
```

The ciphertext computed in the 1000th iteration (CT[1000]) is the result for each of the 100 3-tuples for each selected key size. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.
240 The evaluator shall test the decrypt functionality using the same test as above, exchanging CT and PT, and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

AES-GCM Test

The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

128 bit and 256 bit keys

Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.

Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.

	Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested. The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known. 244 The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation. <u>XTS-AES Test</u> The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths: 256 bit (for AES-128) and 512 bit (for AES-256) keys Three data unit (i.e., plaintext) lengths. One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller. using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt. The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally. The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: AES-CBC # **A498, A497, A499, A494** **C312, C313, C314, C315, C317, C318, C319, C320, C322, C325, C326, C330, C358** CAVP Certs: AES-GCM # **A498** **A497** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.17.3 FCS_COP.1(g) Guidance 1

Objective	If multiple key encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption'** in the AGD to verify that that the method of choosing a specific mode/key size by the end user is described. Upon investigation, the evaluator found that the AGD states: **The TOE supports key encryption and decryption using AES algorithm as specified in ISO/IEC 18033-3. The modes supported are CBC, as specified in ISO/IEC 10116 and GCM, as specified in ISO/IEC 19772. The key size supported is 256 bits.** **Note: The TOE supports AES data encryption and AES decryption by default and no configuration is required.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.17.4 FCS_COP.1(g) KMD 1

Objective	The evaluator shall examine the vendor's KMD to verify that it includes a description of how key encryption will be used as part of the key chain.
Evaluator Findings	The evaluator examined the section titled '**TOE Key Hierarchy'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of how key encryption will be used as part of the key chain. Upon investigation, the evaluator found that the section titled '**TOE Key Hierarchy'** states "The TOE uses PBKDF2 with one round to obtain a key from the user's passcode which in turn is processed by the hardware AES-CBC implementation using the device UID (i.e, Hardware UID/Key)." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.18 FCS_KDF_EXT.1

5.1.18.1 FCS_KDF_EXT.1 TSS 1

Objective	The evaluator shall verify the TSS includes a description of the key derivation function and shall verify the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-108 and SP 800-132.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the key derivation function and verified the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-108 and SP 800-132. Upon investigation, the evaluator found that the TSS states: **The Key derivation function is implemented according to NIST SP 800-132. It leverages the HMAC-SHA-256 algorithm with 50,000 iterations and the UID as the "purpose" value as defined in Appendix A.2.1 of SP 800-132. The Unlock Key is defined as the Boarder Encryption Value (BEV) and is used to unwrap the Class Key with the AES Key Wrap (KW) algorithm.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.1.18.2 FCS_KDF_EXT.1 KMD 1

Objective	The evaluator shall examine the vendor's KMD to ensure that all keys used are derived using an approved method and a description of how and when the keys are derived.
Evaluator Findings	The evaluator examined the section titled '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that all keys used are derived using an approved method and a description of how and when the keys are derived. Upon investigation, the evaluator found that the table in this section states "The Key derivation function is implemented according to NIST SP 800-132. It leverages the HMAC-SHA-256 algorithm with 50,000 iterations and the UID as the "purpose" value as defined in Appendix A.2.1 of SP 800-132." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.19 FCS_KYC_EXT.1

5.1.19.1 FCS_KYC_EXT.1 TSS 1

Objective	The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer 128 bits for products that support only AES128, and no fewer than 256 bits for products that support AES-256.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section contains a high-level description of the BEV sizes that it supports BEV outputs of no fewer 128 bits for products that support only AES128, and no fewer than 256 bits for products that support AES-256. Upon investigation, the evaluator found that the TSS states **TOE supports BEV sizes of 256 bits. The TOE maintains a chain of intermediary keys originating from the BEV to the DEK.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.19.2 FCS_KYC_EXT.1 KMD 1

Objective	The evaluator shall examine the KMD describes a high level description of the key hierarchy for all authorizations methods selected in FCS_AFA_EXT.1 that are used to protect the BEV. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap or key derivation methods that meet FCS_COP.1(d) and FCS_KDF_EXT.1.
Evaluator Findings	The evaluator examined the entirety of the KMD to determine the verdict of this assurance activity. The evaluator confirmed that the KMD provides a high level description of the key hierarchy for all authorizations methods selected in FCS_AFA_EXT.1 that are used to protect the BEV; describes the key chain in detail; and that the key chain maintains a chain of keys using key wrap or key derivation methods that meet FCS_COP.1(d) and FCS_KDF_EXT.1. Upon investigation, the evaluator found that the section titled '**Password**' contains a high level description of the key hierarchy for all authorization methods selected in FCS_AFA_EXT.1 that are used to protect the BEV.

	In addition, the evaluator found that the sections titled '**TOE Key Hierarchy**' and '**TOE Cryptographic Keys**' describe the key chain in detail. Using this information, the evaluator confirmed that a key chain with a strength of 256 bits is maintained using methods that meet FCS_COP.1(d), FCS_COP.1(g) and FCS_KDF_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.19.3 FCS_KYC_EXT.1 KMD 2

Objective	The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the key chain.
Evaluator Findings	The evaluator examined the sections titled '**TOE Key Hierarchy**' and '**TOE Cryptographic Keys**' in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the key chain process functions; includes a diagram illustrating the key hierarchy implemented; details where all keys and keying material is stored or what it is derived from; and ensures that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the key chain. Upon investigation, the evaluator found that the sections titled '**TOE Key Hierarchy**' and '**TOE Cryptographic Keys**' describe how the key chain process functions; include a diagram illustrating the key hierarchy implemented (Figure 2); detail where all keys and keying material is stored or what it is derived from; and ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV (256 bits) is maintained throughout the key chain. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.19.4 FCS_KYC_EXT.1 KMD 3

Objective	The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the strength of keys throughout the key chain. Upon investigation, the evaluator found that the table in this section specifies the strength of keys throughout the key chain. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.20 FCS_KYC_EXT.2

5.1.20.1 FCS_KYC_EXT.2 KMD 1

Objective	The evaluator shall examine the KMD to ensure it describes a high level key hierarchy and details of the key chain. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap or key derivation methods that meet FCS_KDF_EXT.1, FCS_COP.1(d), FCS_COP.1(e), and/or FCS_COP.1(g).
Evaluator Findings	The evaluator examined the entirety of the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes a high level key hierarchy and details of the key chain and that it maintains a chain of keys using key wrap or key derivation methods that meet FCS_KDF_EXT.1, FCS_COP.1(d), FCS_COP.1(e), and/or FCS_COP.1(g). Upon investigation, the evaluator found that the section titled '**TOE Key Hierarchy**' contains a high level description of the key hierarchy (Figure 2). In addition, the evaluator found that the sections titled '**TOE Key Hierarchy**' and '**TOE Cryptographic Keys**' describe the key chain in detail. Using this information, the evaluator confirmed that a key chain with a strength of 256 bits is maintained using methods that meet FCS_COP.1(d), FCS_COP.1(g) and FCS_KDF_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.20.2 FCS_KYC_EXT.2 KMD 2

Objective	The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or knowledge of the BEV and the effective strength of the DEK is maintained throughout the Key Chain.
Evaluator Findings	The evaluator examined the section titled '**Key Management Description'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the key chain process functions; includes a diagram illustrating the key hierarchy implemented; details where all keys and keying material is stored or what it is derived from; ensures that at no point the chain could be broken without a cryptographic exhaust or knowledge of the BEV; and ensures the effective strength of the DEK is maintained throughout the Key Chain. Upon investigation, the evaluator found that Upon investigation, the evaluator found that the sections titled '**TOE Key Hierarchy**' and '**TOE Cryptographic Keys**' describe how the key chain process functions; include a diagram illustrating the key hierarchy implemented (Figure 2); detail where all keys and keying material is stored or what it is derived from; and ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the DEK (256 bits) is maintained throughout the key chain. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.20.3 FCS_KYC_EXT.2 KMD 3

Objective	The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a description of the strength of keys throughout the key chain. Upon investigation, the evaluator found that the table in this section specifies the strength of keys throughout the key chain (256 bits). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.21 FCS_PCC_EXT.1

5.1.21.1 FCS_PCC_EXT.1 TSS 1

Objective	The evaluator shall ensure the TSS describes the manner in which the TOE enforces the construction of passwords, including the length, and requirements on characters (number and type). The evaluator also verifies that the TSS provides a description of how the password is conditioned and the evaluator ensures it satisfies the requirement.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the manner in which the TOE enforces the construction of passwords, including the length, and requirements on characters (number and type); provides a description of how the password is conditioned; and satisfies the requirement. Upon investigation, the evaluator found that the TSS states: **The TOE supports password authentication factor. Passwords of up to 256 characters are supported and can be comprised of any combination of upper-case characters, lower case characters, numbers, and any other 8-bit special character.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.21.2 FCS_PCC_EXT.1 KMD 1

Objective	The evaluator shall examine the KMD to ensure that the formation of the BEV and intermediary keys is described and that the key sizes match that selected by the ST author.
Evaluator Findings	The evaluator examined the section titled '**Password'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that the formation of the BEV and intermediary keys is described and that the key sizes match that selected by the ST author. Upon investigation, the evaluator found that this section states: **To perform password-based key derivation function (PBKDF) operations, the TOE implements PBKDF2 in compliance with NIST SP 800-132. The pseudorandom function (PRF) used is HMAC-SHA-256.** **The TOE uses PBKDF2 with one round to obtain a key from the user's passcode which in turn is processed by the hardware AES-CBC implementation using the device UID (i.e, Hardware UID/Key). The PBKDF2 operation is intended to transform an arbitrary user password into a 256-bit string.** **To generate the salt value used with PBKDF2, the TOE uses its own physical noise source and random number generator. The salt is re-generated every time the passcode changes. The salt value always has a length of 128 bits and is stored in encrypted form within the system keybag. AES is used to encrypt the salt for storage, with the device UID serving as the key.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.21.3 FCS_PCC_EXT.1 KMD 2

Objective	The evaluator shall check that the KMD describes the method by which the password/passphrase is first encoded and then fed to the SHA algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself. The evaluator shall verify that the KMD contains a description of how the output of the hash function is used to form the submask that will be input into the function and is the same length as the BEV as specified above.
Evaluator Findings	The evaluator examined the row '**FCS_AFA_EXT.1/FCS_PCC_EXT.1' of the section titled '**TOE Summary **specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the method by which the password/passphrase is first encoded and then fed to the SHA algorithm; the settings for the algorithm; verify that these are supported by the selections in this component as well as the selections concerning the hash function itself; verify that the KMD contains a description of how the output of the hash function is used to form the submask that will be input into the function and is the same length as the BEV as specified above. Upon investigation, the evaluator found that: **The TOE supports password authentication factor. Passwords of up to 256 characters are supported and can be comprised of any combination of upper-case characters, lower case characters, numbers, and any other 8-bit special character.** **For password-based authentication, the user's password, the TOE's UID and a salt value are used to perform a password-based derivation function (PBKDF2) and derive the Unlock Key. The Unlock Key is defined as the Border Encryption Value (BEV) and is used to unwrap the**

	Class Key with the AES Key Wrap (KW) algorithm. The password is validated if the AES KW function does not return a "Fail" result. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.22 FCS_RBG_EXT.1

5.1.22.1 FCS_RBG_EXT.1 TSS 1

Objective	For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator confirmed that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG and that the TSS identifies the usage of each DRBG mechanism. Upon investigation, the evaluator found that the TSS states: **The TOE performs deterministic random bit generation services according to NIST SP 800-90A] using CTR_DRBG (AES). The SEP TRNG is seeded by 24 ring oscillators. The ring oscillators are constantly inputting new noise data into the conditioner (SHA-256 hash) from which the DRBG seed is obtained. The full entropy of 256 bits is achieved after collecting 285 bits of data from the noise source.** The evaluator also verified that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.22.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary, and provides information regarding how to instantiate/call the DRBG for RBG services needed in this cPP.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption'** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary, and provides information regarding how to instantiate/call the DRBG for RBG services needed in this cPP. Upon investigation, the evaluator found that the AGD states the **TOE performs deterministic random bit generation services according to NIST SP 800-90A using CTR_DRBG (AES).** The evaluator also found a note in the AGD which states, no configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.22.3 FCS_RBG_EXT.1 Test/CAVP 1

Objective	The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions in the operational guidance for configuration of the RNG are valid. 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 shall 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 SP800-90A). 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 shall 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. The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator. Entropy input: the length of the entropy input value must equal the seed length. Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length. Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied. Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.
Evaluator Findings	The evaluator verified that this test activity is addressed by CAVP testing. CAVP Certs: DRBG #**2014, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2028, 2029, C323, C324, C331** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.23 FCS_SNI_EXT.1

5.1.23.1 FCS_SNI_EXT.1 TSS 1

Objective	The evaluator shall ensure the TSS describes how salts are generated. The evaluator shall confirm that the salt is generating using an RBG described in FCS_RBG_EXT.1 or by the

	Operational Environment. If external function is used for this purpose, the TSS should include the specific API that is called with inputs.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how salts are generated using an RBG described in FCS_RBG_EXT.1 or by the Operational Environment. Upon investigation, the evaluator found that the TSS states: **The TOE can generate salts, nonces, and initialization vectors (IVs) using the SEP's DRBG. The DRBG is seeded by the SEP's hardware TRNG. Salts are 16 bytes and are used with the PBKDF2. Nonces are 8 bytes and are used with the trusted update process.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.23.2 FCS_SNI_EXT.1 TSS 2

Objective	The evaluator shall ensure the TSS describes how nonces are created uniquely and how IVs and tweaks are handled (based on the AES mode). The evaluator shall confirm that the nonces are unique and the IVs and tweaks meet the stated requirements.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how nonces are created uniquely and how IVs and tweaks are handled. Upon investigation, the evaluator found that the TSS states the TOE can generate **nonces, and initialization vectors (IVs) using the SEP's DRBG**. **Nonces are 8 bytes and are used with the trusted update process. The IV used with the AES CBC and AES CBC is non-repeating and unpredictable. The TOE enforces that number the number of invocations of GCM does not exceed 2^32 for a given secret key. Tweaks are used with the AES XTS mode of operation. The tweak values should be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer. The tweak value is the physical block number of the media on which the file is being written. This ensures that values cannot be negative. The number is incremented based on the block number values.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24 FCS_VAL_EXT.1

5.1.24.1 FCS_VAL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine which authorization factors support validation.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section states which authorization factors support validation. Upon investigation, the evaluator found that the TSS states **The TOE will validate a BEV using key wrap as specified in FCS_COP.1(d).** **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.2 FCS_VAL_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to review a high-level description if multiple submasks are used within the TOE, how the submasks are validated (e.g., each submask validated before combining, once combined validation takes place).
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section states how the submasks are validated. Upon investigation, the evaluator found that TSS states: **The TOE will validate a BEV using key wrap as specified in FCS_COP.1(d).** **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.3 FCS_VAL_EXT.1 TSS 3

Objective	The evaluator shall also examine the TSS to determine that a subset or all of the authorization factors identified in the SFR can be used to exit from a Compliant power saving state.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section states whether a subset or all of the authorization factors identified in the SFR can be used to exit from a Compliant power saving state. Upon investigation, the evaluator found that the **TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.4 FCS_VAL_EXT.1 Guidance 1

Objective	**(conditional)** If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.
Evaluator Findings	The evaluator examined the section titled '**Validation of Cryptographic Elements'** in the AGD to verify that it describes how to configure the TOE to ensure the limits regarding validation attempts can be established. Upon investigation, the evaluator found that the AGD has detailed configuration steps regarding validation in section titled '**Validation of Cryptographic Elements'** in the AGD. In addition, the evaluator found that the AGD states: **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.5 FCS_VAL_EXT.1 Guidance 2

Objective	**(conditional)** If the validation functionality is specified by the ST author, the evaluator shall examine the operational guidance to ensure that it states the values that the TOE uses for limits regarding validation attempts.
Evaluator Findings	The evaluator examined the section titled '**Validation of Cryptographic Elements'** in the AGD to verify that it states the values that the TOE uses for limits regarding validation attempts. Upon investigation, the evaluator found that the AGD states: **After ten consecutive failed authentication attempts, the TOE blocks the validation attempts by disabling the user account.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.6 FCS_VAL_EXT.1 Guidance 3

Objective	The evaluator shall verify that the guidance documentation states which authorization factors are allowed to exit a compliant power saving state.
Evaluator Findings	The evaluator examined the section titled '**Validation of Cryptographic Elements'** in the AGD to verify that it states which authorization factors are allowed to exit a compliant power saving state. Upon investigation, the evaluator found that the AGD states: **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.7 FCS_VAL_EXT.1 KMD 1

Objective	The evaluator shall examine the KMD to verify that it described the method the TOE employs to limit the number of consecutively failed authorization attempts.
Evaluator Findings	The evaluator examined the section titled '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the method the TOE employs to limit the number of consecutively failed authorization attempts. Upon investigation, the evaluator verified that the KMD describes the method the TOE employs to limit the number of consecutively failed authorization attempts. In addition, the evaluator found that the KMD states: **The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.8 FCS_VAL_EXT.1 KMD 2

Objective	The evaluator shall examine the vendor's KMD to ensure it describes how validation is performed. The description of the validation process in the KMD provides detailed information how the TOE validates the BEV.
Evaluator Findings	The evaluator examined the section titled '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how validation is performed; including detailed information how the TOE validates the BEV. Upon investigation, the evaluator verified that the KMD describes how validation is performed. In addition, the evaluator found that the KMD states: **The TOE will validate a Border Encryption Value using AES KW. The TOE requires the validation of the BEV prior to allowing access to TSF data after exiting a Compliant power saving state and it will block validation after 10 consecutive failed validation attempts. The Unlock Key is defined as the Border Encryption Value (BEV) and is used to unwrap the Class Key with the AES Key Wrap (KW) algorithm. The password is validated if the AES KW function does not return a "Fail" result.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.24.9 FCS_VAL_EXT.1 KMD 3

Objective	The KMD describes how the process works, such that it does not expose any material that might compromise the submask(s).
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the process works, such that it does not expose any material that might compromise the submask(s). Upon investigation, the evaluator verified that the KMD describes how the process works. The evaluator found that the section titled '**TOE Cryptographic Keys'** states: **The Unlock Key is defined as the Border Encryption Value (BEV). It is derived from the UID and user passcode. This key is immediately erased after a successful cryptographic unwrapping of the User Keybag.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS, Guidance and KMD Activities (User Data Protection)

5.2.1 FDP_DSK_EXT.1

5.2.1.1 FDP_DSK_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the disk and the point at which the encryption function is applied. The TSS must make the case that standard methods of accessing the disk drive via the host platforms operating system will pass through these functions.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states: **The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the flash storage and the main memory of the host platform. The T2 chip is placed in the middle of the data path between the Intel chip and the storage disk. The T2 performs the encryption/decryption of the data prior to reaching the Intel chip or the storage. When a read operation is made, the data must first be decrypted by the T2 before the Intel chip has access to the data. When a write operation is made, the data is first encrypted by the T2 and then written to memory as a block of encrypted data. This arrangement ensures that standard methods of accessing the disk drive via the operating system will pass through these functions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FDP_DSK_EXT.1 TSS 2

Objective	For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this functionality.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke the cryptographic functionality provided by the Operational Environment. Upon investigation, the evaluator found that the TSS states: **The T2 provides a dedicated AES crypto engine built into the Direct Memory Access (DMA) path between the flash storage and the main memory of the host platform. The T2 chip is placed in the middle of the data path between the Intel chip and the storage disk. The T2 performs the encryption/decryption of the data prior to reaching the Intel chip or the storage. When a read operation is made, the data must first be decrypted by the T2 before the Intel chip has access to the data. When a write operation is made, the data is first encrypted by the T2 and then written to memory as a block of encrypted data. This arrangement ensures that standard methods of accessing the disk drive via the operating system will pass through these functions. When the host platform is provisioned at first run, the user is prompted to enable the TOE's embedded FDE encryption management program (FileVault 2) and enter a username and password. Once enabled, the storage drive of the host platform remains encrypted and protected from unauthorized access; even if the physical storage device is removed connected to another host platform. The entire storage drive is encrypted.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.3 FDP_DSK_EXT.1 TSS 3

Objective	The evaluator shall verify the TSS in performing the evaluation activities for this requirement. The evaluator shall ensure the comprehensiveness of the description, confirms how the TOE writes the data to the disk drive, and the point at which it applies the encryption function.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that the description is comprehensive, confirms how the TOE writes the data to the disk drive, and the point at which it applies the encryption function. Upon investigation, the evaluator found that the TSS states: **When a write operation is made, the data is first encrypted by the T2 and then written to memory as a block of encrypted data. This arrangement ensures that standard methods of accessing the disk drive via the operating system will pass through these functions.** In addition the **TOE's embedded FDE encryption management program (FileVault 2) and enter a username and password. Once enabled, the storage drive of the host platform remains encrypted and protected from unauthorized access; even if the physical storage device is removed connected to another host platform. The entire storage drive is encrypted with the exception of the following: partition table, Extensible Firmware Interface (EFI) service partition, Apple File System (APFS) container metadata (allocation bitmaps, checkpoint area, EFI jumpstart driver storage, container locker area), recovery volumes, pre-boot volumes, virtual machine (VM) volumes, and CoreDump partitions (if**

	present). Valid credentials are required to be entered before the drive will be decrypted. If the user does not enable FileVault 2 when provisioning the host platform at first run, FileVault 2 can be enabled later through the Security & Privacy menu available via the host platform. By default, the host platform's storage drive is always encrypted. The TOE cryptographic key management changes after enabling FileVault 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.4 FDP_DSK_EXT.1 TSS 4

Objective	The evaluator shall verify that the TSS describes the initialization of the TOE and the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE. The evaluator shall verify the TSS describes areas of the disk that it does not encrypt (e.g., portions associated with the Master Boot Records (MBRs), boot loaders, partition tables, etc.). If the TOE supports multiple disk encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all storage devices on the platform.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section TSS describes the initialization of the TOE; the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE; describes areas of the disk that it does not encrypt; and if the TOE supports multiple disk encryptions, encrypts all storage devices on the platform during the initialization procedure. Upon investigation, the evaluator found that the TSS states: **When the host platform is provisioned at first run, the user is prompted to enable the TOE's embedded FDE encryption management program (FileVault 2) and enter a username and password. Once enabled, the storage drive of the host platform remains encrypted and protected from unauthorized access; even if the physical storage device is removed connected to another host platform. The entire storage drive is encrypted with the exception of the following: partition table, Extensible Firmware Interface (EFI) service partition, Apple File System (APFS) container metadata (allocation bitmaps, checkpoint area, EFI jumpstart driver storage, container locker area), recovery volumes, pre-boot volumes, virtual machine (VM) volumes, and CoreDump partitions (if present). Valid credentials are required to be entered before the drive will be decrypted. If the user does not enable FileVault 2 when provisioning the host platform at first run, FileVault 2 can be enabled later through the Security & Privacy menu available via the host platform. By default, the host platform's storage drive is always encrypted. The TOE cryptographic key management changes after enabling FileVault 2.** Additionally, the AGD section titled **'Enable Full Disk Encryption'** and **'Changing User Passwords'** describes the initialization procedure encrypts all storage devices on the platform. In addition, the TSS also states: **A recovery key is a randomly generated 28-character code that the user can use to reset their password. The recovery key is generated during the process and manually saved by the user. The recovery key is never stored in the TOE. The recovery key is hashed (SHA-256) and the resulting value is stored in the T2. If FileVault is disabled and re-enabled, a new recovery key is generated.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.1.5 FDP_DSK_EXT.1 Guidance 1

Objective	The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the FDE function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient, on all platforms, to ensure that all hard drive devices will be encrypted when encryption is enabled.
Evaluator Findings	The evaluator examined the section titled '**Enable Full Disk Encryption'** in the AGD to verify that it describes the initial steps needed to enable the FDE function, including any necessary preparatory steps, and that the instructions are sufficient, on all platforms, to ensure that all hard drive devices will be encrypted when encryption is enabled. Upon investigation, the evaluator found that the AGD describes detail descriptive explanation and instructions to enable the FDE function, Mac platforms with FileVault to ensure that all hard drive devices will be encrypted when encryption is enabled. The section titled 'Enable Full Disk Encryption' in the AGD also states: **In Mac OS X 10.3 or later, Mac computers provide FileVault, a built-in encryption capability to secure all data at rest. FileVault uses the AES-XTS data encryption algorithm to protect full volumes on internal and removable storage devices. On Mac computers with the Apple T2 Security Chip, encrypted internal storage devices directly connected to the T2 chip leverage the hardware security capabilities of the chip. After a user turns on FileVault on a Mac, their credentials are required during the boot process.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.6 FDP_DSK_EXT.1 KMD 1

Objective	The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions associated with the Master Boot Record (MBRs), partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the device's host interface and the device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.
Evaluator Findings	The evaluator examined the section titled '**Apple File System (APFS) encrypted storage'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section • includes a description of the data encryption engine, its components, and details about its implementation; • provides a functional (block) diagram showing the main components and the data path;

	• shows the location of the data encryption engine within the data path; • contains enough detail showing the main components within the data path; • and clearly identifies the data encryption engine. Upon investigation, the evaluator found that: • The KMD provides this detailed description of the data encryption engine: **"The Apple T2 security chip is a system on chip (SoC) that contains a separate processing element used for cryptographic functions, the Apple Secure Enclave consisting of the sepOS and the isolated Secure Enclave Processor (SEP). The Secure Enclave contains the Secure Key Store (SKS) cryptographic module for performing cryptographic operations, key generation (using its internal hardware true random number generator) and key storage required for the TOE to perform full drive encryption.** **The T2 chip has a dedicated AES encryption engine built into the Direct Memory Access (DMA) path between the flash storage and the main memory of the host platform. The Secure Enclave is responsible for performing the key management for encryption and/or decryption of the data prior to reaching macOS running on the Intel chip or the storage volume.** • The KMD includes a functional block diagram (Figure 1) showing the main components including the Secure Enclave AES Engine. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.7 FDP_DSK_EXT.1 KMD 2

Objective	The evaluator shall verify the KMD provides sufficient instructions for all platforms to ensure that when the user enables encryption, the product encrypts all hard storage devices. The evaluator shall verify that the KMD describes the data flow from the device's host interface to the device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area).
Evaluator Findings	The evaluator examined the section titled '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section provides sufficient instructions for all platforms to ensure that when the user enables encryption, the product encrypts all hard storage devices; describes the data flow from the device's host interface to the device's persistent media storing the data; and provides information on those conditions in which the data bypasses the data encryption engine. Upon investigation, the evaluator found that: **For Macs with T2 chip, the data on the SSD is always encrypted using a hardware-accelerated AES engine built into the T2 chip. This encryption is performed with 256-bit keys tied to a unique identifier within the T2 chip. When a user enables FileVault on their Mac their credentials are required during the boot process. Without valid login credentials, the internal Apple File System or APFS volume remains encrypted and is protected from unauthorized access even if the physical storage device is removed and connected to another computer. Users can only access data after authenticating to the TOE which requires that the encryption engine is fully initialized, and an AES Key Wrap (KW) operation**

	is performed. This process prevents the transfer of user data before the encryption engine is fully initialized. **The TOE does not encrypt the following APFS volumes:** **1. Pre-boot,** **2. Recovery and** **3. Virtual Memory paging partition.** **When a Mac computer with the Apple T2 Security Chip chip is turned on, the chip executes code from read-only memory known as 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.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.8 FDP_DSK_EXT.1 KMD 3

Objective	The evaluator shall verify that the KMD provides a description of the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption. The evaluator shall validate that the product does not allow for the transfer of user data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.
Evaluator Findings	The evaluator examined the sections titled '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements**' and '**TOE Secure Boot Process'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section provides a description of the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption; indicates that the product does not allow for the transfer of user data before it fully initializes the encryption; and indicates that the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key. Upon investigation, the evaluator found that the '**TOE Secure Boot Process'** section states: **When a Mac computer with the Apple T2 Security Chip chip is turned on, the chip executes code from read-only memory known as 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.** In addition, the '**CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E KMD Requirements**' section states: **Users can only access data after authenticating to the TOE which requires that the encryption engine is fully initialized, and an AES Key Wrap (KW) operation is performed.**

	This process prevents the transfer of user data before the encryption engine is fully initialized. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS, Guidance and KMD Activities (Security Management)

5.3.1 FMT_MOF.1

5.3.1.1 FMT_MOF.1 TSS 1

Objective	If support for Compliant power saving state(s) are claimed in the ST, the evaluator shall ensure the TSS describes how these are managed and shall ensure that TSS describes how only privileged users (administrators) are allowed to manage the states.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how Compliant power saving state(s) are managed and how only privileged users (administrators) are allowed to manage the states. Upon investigation, the evaluator found that the TSS states the **TOE restricts the ability to modify the behavior of complaint power saving state to authorized users.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FMT_MOF.1 Guidance 1

Objective	The evaluator to check if guidance documentation describes which authorization factors are required to change Compliant power saving state behavior and properties.
Evaluator Findings	The evaluator examined the section titled '**Authorization Factors'** in the AGD to verify that it describes which authorization factors are required to change Compliant power saving state behavior and properties. Upon investigation, the evaluator found that the AGD states: **The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. In order to resume from a compliant power state, the user must re-authenticate to the TOE. The user can authenticate using username and password.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2 FMT_SMF.1(1)

5.3.2.1 FMT_SMF.1(1) TSS 1

Objective	If item a) [forwarding requests to change the DEK to the EE] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE sends the request to the EE to change the DEK.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE sends the request to the EE to change the DEK. Upon investigation, the evaluator found that the TSS states: • **Forwarding requests to change the DEK to the EE,** • **The Volume Key is defined as the Data Encryption Key (DEK). It is randomly generated when a user volume is created, and the key is destroyed by issuing an authenticated command by a single overwrite consisting of zeroes.** • **The DEK is the Volume key which is created for each volume at volume creation time.** • **The user can destroy the Volume key by destroying/erasing the volume. This option can be selected after authenticating to the TOE and the TOE performs a cryptographic erase of the keying material.** • **The above can be achieved by starting the Disk Utility application and then selecting the appropriate volume to be erased.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.2 FMT_SMF.1(1) TSS 2

Objective	If item b) [forwarding requests to cryptographically erase the DEK to the EE] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE sends the request to the EE to cryptographically erase the DEK.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE sends the request to the EE to cryptographically erase the DEK. Upon investigation, the evaluator found that the TSS states: • **Forwarding requests to cryptographically erase the DEK to the EE** • **The Volume Key is defined as the Data Encryption Key (DEK). It is randomly generated when a user volume is created, and the key is destroyed by issuing an authenticated command by a single overwrite consisting of zeroes.** • **The DEK is the Volume key which is created for each volume at volume creation time.** • **The user can destroy the Volume key by destroying/erasing the volume. This option can be selected after authenticating to the TOE and the TOE performs a cryptographic erase of the keying material.** • **The above can be achieved by starting the Disk Utility application and then selecting the appropriate volume to be erased.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.3 FMT_SMF.1(1) TSS 3

Objective	If item c) [allowing authorized users to change authorization factors or set of authorization factors used] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the methods by which users may change the set of all authorization factor values supported.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the methods by which users may change the set of all authorization factor values supported. Upon investigation, the evaluator found that the TSS states: • **allowing authorized users to change authorization factors or set of authorization factors used** • **Once the user successfully authenticates to the TOE, the TOE can be configured to change the authorization factors that can be used: password.** • **The above can be achieved by navigating to System Preferences-> Users & Groups -> Select the appropriate user -> Change Password.** • **configure authorization factors** • **Once the user successfully authenticates to the TOE, the TOE can be configured to change the authorization factors that can be used: password.** • **The above can be achieved by navigating to System Preferences-> Users & Groups -> Select the appropriate user -> Change Password.** In addition, the evaluator found that the TSS describes the methods by which users may change the set of all authorization factor values supported. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.4 FMT_SMF.1(1) TSS 4

Objective	If item d) [initiate TOE firmware/software updates] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the process to initiate TOE firmware/software updates. Upon investigation, the evaluator found that the TSS states: • **initiate TOE firmware/software updates** • **The user must successfully login to the TOE before initiating a TOE firmware/software update. After successfully authenticating to the TOE, the user manually downloads the TOE software update(s) from** https://support.apple.com/downloads**.** • **Once the update(s) is downloaded, the user needs to initiate the TOE update process by double clicking or right-click -> Open the downloaded update.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.5 FMT_SMF.1(1) TSS 5

Objective	If item e) is selected in FMT_SMF.1.1: If power saving states can be managed, the evaluator shall ensure that the TSS describes how this is performed, including how the TOE supports disabling certain power saving states if more than one are supported. If additional management functions are claimed in the ST, the evaluator shall ensure the TSS describes the additional functions.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. The evaluator found that FMT_SMF.1.1: If power saving states can be managed is not selected. In addition, the evaluator also examined the section titled **'TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the additional functions. Upon investigation, the evaluator found that the following additional functions were selected and described: • **configure authorization factors** The evaluator found that the TSS states: • **Once the user successfully authenticates to the TOE, the TOE can be configured to change the authorization factors that can be used: password.** • **The above can be achieved by navigating to System Preferences-> Users & Groups -> Select the appropriate user -> Change Password.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.6 FMT_SMF.1(1) Guidance 1

Objective	If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how the functions for A and B can be initiated by the user.

Evaluator Findings	The evaluator examined the section titled '**TOE Management Functions'** in the AGD to verify that it describes how the functions for A and B can be initiated by the user. Upon investigation, the evaluator found that the AGD states:
	
	• **Forward a command to the Encryption Engine (EE) to change and cryptographically erase the Device Encryption Key or DEK.**
	  ○ **Open the Disk Utility application, and select the disk to be encrypted. In this case, the name of the disk was set to FDP_DSK_EXT1 drive.**
	  ○ **Note: FDP_DSK_EXT1 is an example disk name. For further information on Disk Utility, refer Disk Utility User Guide: https://support.apple.com/guide/disk-utility/welcome/mac**
	  ○ **Then select "Mac OS Extended (Journaled, Encrypted)".**
	  ○ **Click Erase.**
	
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3.2.7 FMT_SMF.1(1) Guidance 2

Objective	If item c) [allowing authorized users to change authorization factors or set of authorization factors used] is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how selected authorization factor values are changed.

Evaluator Findings	The evaluator examined the section titled **'TOE Management Functions'** in the AGD to verify that it describes how selected authorization factor values are changed. Upon investigation, the evaluator found that the AGD states:
	• **Allowing authorized users to change authorization factors such as a user password.**
	  • **Login to the TOE as an authorized user:**
	  • **Navigate to System Preferences -> Users & Groups.**
	  • **Click on Change Password.**
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3.2.8 FMT_SMF.1(1) Guidance 3

Objective	If item d) [initiate TOE firmware/software updates] is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how to initiate TOE firmware/software updates.
Evaluator Findings	The evaluator examined the section titled **'TOE Management Functions'** in the AGD to verify that it describes how to initiate TOE firmware/software updates. Upon investigation, the evaluator found that the AGD states: • **Initiate the TOE firmware/software update (refer to** Section 'Installing Updates**').** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.9 FMT_SMF.1(1) Guidance 4

Objective	If item e) is selected in FMT_SMF.1.1: Default Authorization Factors: It may be the case that the TOE arrives with default authorization factors in place. If it does, then the selection in section E must be made so that there is a mechanism to change these authorization factors. The operational guidance shall describe the method by which the user changes these factors when they are taking ownership of the device. The TSS shall describe the default authorization factors that exist.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that in FMT_SMF.1.1: Default Authorization Factors is not selected. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.2.10 FMT_SMF.1(1) Guidance 5

Objective	If item e) is selected in FMT_SMF.1.1: Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that FMT_SMF.1.1: Disable Key Recovery is not selected. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.2.11 FMT_SMF.1(1) Guidance 6

Objective	If item e) is selected in FMT_SMF.1.1: Power Saving: The guidance shall describe the power saving states that are supported by the TSF, how these states are applied, how to configure when these states are applied (if applicable), and how to enable/disable the use of specific power saving states (if applicable).
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that FMT_SMF.1.1: Power Saving is not selected. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.3 FMT_SMF.1(2)

5.3.3.1 FMT_SMF.1(2) TSS 1

Objective	If item a) [change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE changes the DEK.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE changes the DEK. Upon investigation, the evaluator found that the TSS states: • **Authorization Acquisition and Encryption Engine** • **Forwarding requests to change the DEK to the Encryption Engine.** • **Forwarding requests to cryptographically erase the DEK to the Encryption Engine.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.2 FMT_SMF.1(2) TSS 2

Objective	If item b) [erase the DEK, as specified in FCS_CKM.4(a)] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE cryptographically erases the DEK.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE cryptographically erases the DEK. Upon investigation, the evaluator found that the TSS states: • **Forwarding requests to cryptographically erase the DEK to the Encryption Engine.** • **configure cryptographic functionality** • **The Volume Key is defined as the Data Encryption Key (DEK). It is randomly generated when a user volume is created, and the key is destroyed by issuing an authenticated command by a single overwrite consisting of zeroes.** • **The DEK is the Volume key which is created for each volume at volume creation time.** • **The user can destroy the Volume key by destroying/erasing the volume. This option can be selected after authenticating to the TOE and the TOE performs a cryptographic erase of the keying material.** • **The above can be achieved by starting the Disk Utility application and then selecting the appropriate volume to be erased.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.3 FMT_SMF.1(2) TSS 3

Objective	If item c) [initiate TOE firmware/software updates] is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that [initiate TOE firmware/software updates] is selected in FMT_SMF.1.1 and the section titled '**TOE Summary Specification'** in the Security Target describes the process to initiate TOE firmware/software updates. Upon investigation, the evaluator found that the TSS states: • **initiate TOE firmware/software updates** • **The user must successfully login to the TOE before initiating a TOE firmware/software update. After successfully authenticating to the TOE, the user manually downloads the TOE software update(s) from https://support.apple.com/downloads.** • **Once the update(s) is downloaded, the user needs to initiate the TOE update process by double clicking or right-click -> Open the downloaded update.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.4 FMT_SMF.1(2) TSS 4

Objective	If item d) is selected in FMT_SMF.1.1: If additional management functions are claimed in the ST, the evaluator shall ensure the TSS describes the additional functions.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. The evaluator found that no additional management functions are claimed. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.3.5 FMT_SMF.1(2) Guidance 1

Objective	If item a) [change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded] is selected in FMT_SMF.1.1: The evaluator shall review the AGD guidance and shall determine that the instructions for changing a DEK exist. The instructions must cover all environments on which the TOE is claiming conformance, and include any preconditions that must exist in order to successfully generate or re-generate the DEK.

Evaluator Findings	The evaluator examined the section titled **'TOE Management Functions'** in the AGD to verify that the instructions for changing a DEK exist, that they cover all environments on which the TOE is claiming conformance, and include any preconditions that must exist in order to successfully generate or re-generate the DEK. Upon investigation, the evaluator found that the AGD states:
	
	• **Forward a command to the Encryption Engine (EE) to change and cryptographically erase the Device Encryption Key or DEK.**
	  ○ **Open the Disk Utility application, and select the disk to be encrypted. In this case, the name of the disk was set to FDP_DSK_EXT1 drive.**
	  ○ **Note: FDP_DSK_EXT1 is an example disk name. For further information on Disk Utility, refer Disk Utility User Guide: https://support.apple.com/guide/disk-utility/welcome/mac**
	  ○ **Then select "Mac OS Extended (Journaled, Encrypted)".**
	  ○ **Click Erase.**
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3.3.6 FMT_SMF.1(2) Guidance 2

Objective	If item c) [initiate TOE firmware/software updates] is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how to initiate TOE firmware/software updates.
Evaluator Findings	The evaluator examined the section titled **'TOE Management Functions'** in the AGD to verify that it describes how to initiate TOE firmware/software updates. Upon investigation, the evaluator found that the AGD states: • **Initiate the TOE firmware/software update (refer to Section 7 Installing Updates).** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.7 FMT_SMF.1(2) Guidance 3

Objective	If item d) is selected in FMT_SMF.1.1: Default Authorization Factors: It may be the case that the TOE arrives with default authorization factors in place. If it does, then the selection in item D must be made so that there is a mechanism to change these authorization factors. The operational guidance shall describe the method by which the user changes these factors when they are taking ownership of the device. The TSS shall describe the default authorization factors that exist.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that [Default Authorization Factors] is not selected. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.3.8 FMT_SMF.1(2) Guidance 4

Objective	If item d) is selected in FMT_SMF.1.1: Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that [Disable Key Recovery] is not selected. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.3.3.9 FMT_SMF.1(2) KMD 1

Objective	If item d) is selected in FMT_SMF.1.1: If the TOE offers the functionality to import an encrypted DEK, the evaluator shall ensure the KMD describes how the TOE imports a wrapped DEK and performs the decryption of the wrapped DEK.
Evaluator Findings	The evaluator examined the SFR in the Security Target to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the functionality to import an encrypted DEK is not offered. Based on these findings, this assurance activity is considered non-applicable.
Verdict	Pass

5.4 TSS, Guidance and KMD Activities (Protection of the TSF)

5.4.1 FPT_FAC_EXT.1

5.4.1.1 FPT_FAC_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes information stating how the Access Control process takes place along with a description of the values that are used.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes information stating how the Access Control process takes place along with a description of the values that are used. Upon investigation, the evaluator found that the TSS states:

	The user must successfully login to the TOE before initiating a TOE software/firmware update. Only authorized users i.e. privileged/non-privileged users can initiate the TOE update process. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 FPT_FAC_EXT.1 Guidance 1

Objective	The evaluator ensures that the Operational Guidance describes how the user will be expected to interact with the authorization process.
Evaluator Findings	The evaluator examined the section titled '**TOE Management Functions'** and **'Authorization Factors'** in the AGD to verify that it describes how the user will be expected to interact with the authorization process. Upon investigation, the evaluator found that the AGD describes instructional authorization process and the AGD also states: **Allowing authorized users to change authorization factors or set of authorization factors used**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.2 FPT_FUA_EXT.1

5.4.2.1 FPT_FUA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes how the TOE uses the RTU, what type of key or hash value, and where the value is stored on the RTU. The evaluator shall also verify that the TSS contains a description (storage location) of where the original firmware exists.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes how the TOE uses the RTU, what type of key or hash value, and where the value is stored on the RTU; and contains a description (storage location) of where the original firmware exists. Upon investigation, the evaluator found that the TSS states: **A vendor-controlled server is leveraged for obtaining firmware update code packages. The code packages containing the macOS, T2 OS/firmware, and SEP OS/firmware are all bundled together. The firmware/OS is stored within the T2 chip. The TOE stores the incoming update in a temporary location on flash. Once the transfer is complete, the SEP verifies the RSA 2048-bit digital signature verification. If the verification is successful, the TOE installs the update and reboots the host device. If the verification is unsuccessful, the TOE terminates the updates process.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3 FPT_KYP_EXT.1

5.4.3.1 FPT_KYP_EXT.1 TSS 1 [TD0458]

Objective	The evaluator shall examine the TSS and verify it identifies the methods used to protect keys stored in non-volatile memory.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section identifies the methods used to protect keys stored in non-volatile memory. Upon investigation, the evaluator found that the TSS states: **The TOE leverages NAND flash for non-volatile memory. All symmetric keys that are persistently stored, except for the UID, are wrapped in NAND flash. The UID is fused into the SEP's ROM is not accessible by any component outside of the SEP and cannot be erased.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.2 FPT_KYP_EXT.1 KMD 1 [TD0458]

Objective	The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in non-volatile memory. The description of the key chain shall be reviewed to ensure the selected method is followed for the storage of wrapped or encrypted keys in non-volatile memory and plaintext keys in non-volatile memory meet one of the criteria for storage.
Evaluator Findings	The evaluator examined the section titled '**TOE Cryptographic Keys'** in the KMD to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the storage location of all keys and the protection of all keys stored in non-volatile memory, and that the selected method is followed for the storage of wrapped or encrypted keys in non-volatile memory and plaintext keys in non-volatile memory meet one of the criteria for storage. Upon investigation, the evaluator found that the section titled '**TOE Cryptographic Keys'** describes the storage location of all keys and the protection of all keys stored in non-volatile memory. In addition, the evaluator determined the following criteria is used for storage of keys in non-volatile memory: • The plaintext UID "**can't be read by firmware or software, and it's used only by the processor's hardware AES Engine**." • The Class A and Volume keys are wrapped when stored. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4 FPT_PWR_EXT.1

5.4.4.1 FPT_ PWR_EXT.1 TSS 1

Objective	The evaluator shall validate the TSS contains a list of Compliant power saving states.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section contains a list of Compliant power saving states. Upon investigation, the evaluator found that the TSS states: **The TOE supports the following power savings state: G2(S5)-soft off. The TOE can enter G2(S5)-soft off power savings state by the user selecting Shutdown option on the TOE host device.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.4.2 FPT_PWR_EXT.1 Guidance 1 [TD0460]

Objective	The evaluator shall ensure that guidance documentation contains a list of Compliant power saving states. If additional power saving states are supported, then the evaluator shall validate that the guidance documentation states how non-Compliant power states are disabled.
Evaluator Findings	The evaluator examined the section titled '**Authorization Factors'** in the AGD to verify that it contains a list of Compliant power saving states, and if additional power saving states are supported, states how non-Compliant power states are disabled. Upon investigation, the evaluator found that the AGD states: **The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. In order to resume from a compliant power state, the user must re-authenticate to the TOE. The user can authenticate using username and password.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.5 FPT_PWR_EXT.2

5.4.5.1 FPT_PWR_EXT.2 TSS 1

Objective	The evaluator shall validate that the TSS contains a list of conditions under which the TOE enters a Compliant power saving state.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section contains a list of conditions under which the TOE enters a Compliant power saving state. Upon investigation, the evaluator found that the TSS states: **The TOE supports the following power savings state: G2(S5)-soft off. The TOE can enter G2(S5)-soft off power savings state by the user selecting Shutdown option on the TOE host device.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.5.2 FPT_PWR_EXT.2 Guidance 1

Objective	The evaluator shall check that the guidance contains a list of conditions under which the TOE enters a Compliant power saving state. Additionally, the evaluator shall verify that the guidance documentation states whether unexpected power-loss events may result in entry to a non-Compliant power saving state and, if that is the case, validate that the documentation contains information on mitigation measures.
Evaluator Findings	The evaluator examined the section titled **'Authorization Factors'** in the AGD to verify that it contains a list of conditions under which the TOE enters a Compliant power saving state, states whether unexpected power-loss events may result in entry to a non-Compliant power saving state and, if that is the case, contains information on mitigation measures. Upon investigation, the evaluator found that the AGD **The TOE supports the following power saving state: G2(S5)- soft off, also recognized as Shutdown. The TOE can enter G2(S5)-soft off power saving state by the user selecting the Shutdown option on the TOE host device. In order to resume from a compliant power state, the user must re-authenticate to the TOE by using a correct username and password.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.6 FPT_TST_EXT.1

5.4.6.1 FPT_TST_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the known-answer self-tests for cryptographic functions.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes the known-answer self-tests for cryptographic functions. Upon investigation, the evaluator found that the TSS states known answer tests (KATs) are: • **CTR_DRBG with ASE 256: The TOE instantiates the DRBG with a known value, invokes the generate function, and compares the generated bits to the expected bits. This satisfies the SP 800-90Ar1 Section 11.3 Health Tests by showing the correct operation of the seed, reseed, and generate functions.** • **RSA 2048 with SHA-256 Signature Verification: satisfied by the Firmware Integrity signature verification test above.** • **RSA 2048 with SHA-256 Encrypt/Decrypt** • **HMAC-SHA-256: MAC generation with a known key and message.** • **AES 128 XTS Encrypt/Decrypt: This shows the correct operation of AES Encrypt and Decrypt primitive functions with a 256-bit key.** • **AES CBC 256-bit encrypt and decrypt KATs** • **AES GCM 256-bit encrypt and decrypt KATs** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.6.2 FPT_TST_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TOE and the method by which the TOE tests those functions. The evaluator shall verify that the TSS includes each of these functions, the method by which the TOE verifies the correct operation of the function. The evaluator shall verify that the TSF data are appropriate for TSF Testing. For example, more than blocks are tested for AES in CBC mode, output of AES in GCM mode is tested without truncation, or 512-bit key is used for testing HMAC-SHA-512.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes, for some set of non-cryptographic functions affecting the correct operation of the TOE, the method by which the TOE tests those functions; describes the method by which the TOE verifies the correct operation of the function for TSF data that are appropriate for TSF Testing. Upon investigation, the evaluator found that the TSS states: **During power-up, the TOE performs a signature verification of firmware and software using the Apple Root CA Public Key. When the host device is powered-on, the SEP initiates the Secure Boot process. The SEP's Boot ROM first authenticates the signature of the Bridge Boot code (T2 Boot ROM code). If the verifications fails, the TOE returns an error and enters the Device Firmware Upgrade (DFU) mode; requiring a correct update to continue. If the verification is successful, the Bridge Boot code then authenticates the signature of the T2 kernel cache. The T2 kernel cache then authenticates the signature of the Unified Extensible Firmware Interface (UEFI) firmware. The UEFI firmware is then used to authenticate the boot.efi file within the Intel processor of the TOE host device. The boot.efi file then authenticates the macOS immutable kernel. The macOS then authenticates third party kernel extensions (kexts) and OS Userspace.** In addition the TSS also states: **The TOE performs the following known answer tests (KATs) to verify the correct operation of the cryptographic functions:** • **CTR_DRBG with ASE 256: The TOE instantiates the DRBG with a known value, invokes the generate function, and compares the generated bits to the expected bits.** • **RSA 2048 with SHA-256 Signature Verification: satisfied by the Firmware Integrity signature verification test above.** • **RSA 2048 with SHA-256 Encrypt/Decrypt** • **HMAC-SHA-256: MAC generation with a known key and message.** • **AES 128 XTS Encrypt/Decrypt: This shows the correct operation of AES Encrypt and Decrypt primitive functions with a 256-bit key.** • **AES CBC 256-bit encrypt and decrypt KATs** • **AES GCM 256-bit encrypt and decrypt KATs** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.6.3 FPT_TST_EXT.1 TSS 3

Objective	If FCS_RBG_EXT.1 is implemented by the TOE and according to NIST SP 800-90, the evaluator shall verify that the TSS describes health tests that are consistent with section 11.3 of NIST SP 800-90.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes health tests that are consistent with section 11.3 of NIST SP 800-90. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.6.4 FPT_TST_EXT.1 TSS 4

Objective	If any FCS_COP functions are implemented by the TOE, the TSS shall describe the known-answer self-tests for those functions.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describe the known-answer self-tests for those functions. Upon investigation, the evaluator found that the TSS states: ○ **CTR_DRBG with ASE 256: The TOE instantiates the DRBG with a known value, invokes the generate function, and compares the generated bits to the expected bits.** ○ **RSA 2048 with SHA-256 Signature Verification: satisfied by the Firmware Integrity signature verification test above.** ○ **RSA 2048 with SHA-256 Encrypt/Decrypt** ○ **HMAC-SHA-256: MAC generation with a known key and message.** ○ **AES 128 XTS Encrypt/Decrypt: This shows the correct operation of AES Encrypt and Decrypt primitive functions with a 256-bit key.** ○ **AES CBC 256-bit encrypt and decrypt KATs** ○ **AES GCM 256-bit encrypt and decrypt KATs** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.6.5 FPT_TST_EXT.1 TSS 5

Objective	The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TSF, the method by which those functions are tested. The TSS will describe, for each of these functions, the method by which correct operation of the function/component is verified. The evaluator shall determine that all of the identified functions/components are adequately tested on startup.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes, for some set of non-cryptographic functions affecting the correct operation of the TSF, the method by which those functions are tested; for each of these functions, describes the method by which correct operation of the function/component is verified; and ensures that all of the identified functions/components are adequately tested on startup. Upon investigation, the evaluator found that the TSS states: **During power-up, the TOE performs a signature verification of firmware and software using the Apple Root CA Public Key. When the host device is powered-on, the SEP initiates the Secure Boot process. The SEP's Boot ROM first authenticates the signature of the Bridge Boot code (T2 Boot ROM code). If the verifications fails, the TOE returns an error and enters the Device Firmware Upgrade (DFU) mode; requiring a correct update to continue. If the verification is successful, the Bridge Boot code then authenticates the signature of the T2 kernel cache. The T2 kernel cache then authenticates the signature of the Unified Extensible Firmware Interface (UEFI) firmware. The UEFI firmware is then used to authenticate the boot.efi file within the Intel processor of the TOE host device. The boot.efi file then authenticates the macOS immutable kernel. The macOS then authenticates third party kernel extensions (kexts) and OS Userspace.** The evaluator also found that TOE performs the known answer tests (KATs) to verify the correct operation of the cryptographic functions is listed in the TSS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.7 FPT_TUD_EXT.1

5.4.7.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes information stating that an authorized source signs TOE updates and will have an associated digital signature. The evaluator shall examine the TSS contains a definition of an authorized source along with a description of how the TOE uses public keys for the update verification mechanism in the Operational Environment. The evaluator ensures the TSS contains details on the protection and maintenance of the TOE update credentials.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes information stating that an authorized source signs TOE updates and will have an associated digital signature; contains a definition of an authorized source along with a description of how the TOE uses public keys for the update verification mechanism in the Operational Environment; and contains details on the protection and maintenance of the TOE update credentials. Upon investigation, the evaluator found that the TSS states: **The SEP verifies the RSA 2048-bit digital signature verification. If the verification is successful, the TOE installs the update and reboots the host device. If the verification is unsuccessful, the TOE terminates the updates process.** **The user must successfully login to the TOE before initiating a TOE software/firmware update. Only authorized users i.e. privileged/non-privileged users can initiate the TOE update process.** Once the transfer is complete, the SEP verifies the RSA 2048-bit digital signature verification. If the verification is successful, the TOE installs the update and reboots the host device. If the verification is unsuccessful, the TOE terminates the updates process. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.7.2 FPT_TUD_EXT.1 TSS 2

Objective	If the Operational Environment performs the signature verification, then the evaluator shall examine the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this cryptographic functionality.
Evaluator Findings	The evaluator examined the section titled '**TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this cryptographic functionality. Upon investigation, the evaluator found that the TSS states: **A vendor-controlled server is leveraged for obtaining firmware update code packages. The code packages containing the macOS, T2 OS/firmware, and SEP OS/firmware are all bundled together. The firmware/OS is stored within the T2 chip. The TOE stores the incoming update in a temporary location on flash. Once the transfer is complete, the SEP verifies the RSA 2048-bit digital signature verification. If the verification is successful, the TOE installs the update and reboots the host device. If the verification is unsuccessful, the TOE terminates the updates process.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.4.7.3 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator ensures that the operational guidance describes how the TOE obtains vendor updates to the TOE; the processing associated with verifying the digital signature of the updates (as defined in FCS_COP.1(a)); and the actions that take place for successful and unsuccessful cases.
Evaluator Findings	The evaluator examined the section titled '**Installing Updates'** in the AGD to verify that it describes how the TOE obtains vendor updates to the TOE; the processing associated with verifying the digital signature of the updates (as defined in FCS_COP.1(a)); and the actions that take place for successful and unsuccessful cases. Upon investigation, the evaluator found that the AGD states: **Authentic OS and software application updates can be downloaded from https://support.apple.com/downloads. Once an update(s) is downloaded, the user can initiate the installation of that update in the following manner:** • **Download the appropriate update from https://support.apple.com/downloads according to the user requirement(s).** • **Double click on the downloaded update.** • **The TOE verifies the integrity of the software update by performing an RSA 2048-bit digital signature verification.** • **After the digital signature verification is successful the TOE will install the update.** • **If the digital signature verification fails, the TOE will warn the user that the digital signature verification failed and will not install the update. The TOE then terminates the update process.** **Note: For OS updates, the TOE may occasionally reboot itself during the update process. This behavior is not uncommon. Software Application updates may or may not require the TOE to reboot.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1.1 FCS_AFA_EXT.1 [AA]

Item	Data
Test Assurance Activity	The password authorization factor is tested in FCS_PCC_EXT.1. Test 1 (conditional): If there is more than one authorization factor, ensure that failure to supply a required authorization factor does not result in access to the decrypted plaintext data.

Test Steps	• Verify that the data is encrypted by the TOE. (in case of macOS Catalina 10.15 it is FileVault Encryption)
	• For Password:
	  ○ Attempt to login to the TOE using correct password
	  ○ Verify that the TOE grants access to the decrypted plaintext data.
	  ○ Attempt to login to the TOE without inputting the password.
	  ○ Verify that the TOE prevents the user from accessing the decrypted plaintext data.

Expected Test Results	• Verify that the data is encrypted by the TOE. (in case of macOS Catalina 10.15 it is FileVault Encryption)
	• For Password:
	  ○ Attempt to login to the TOE using correct password
	• Verify that the TOE grants access to the decrypted plaintext data.
	  ○ Attempt to login to the TOE without inputting the password and
	  ○ Verify that the TOE prevents the user from accessing the decrypted plaintext data.

Pass/Fail with Explanation	Pass. The TOE ensures that only valid authorization factors result in accessing the decrypted plaintext data.

6.1.2 FCS_AFA_EXT.2 [AA]

Item	Data
Test Assurance Activity	The evaluator shall examine the TSS for a description of authorization factors and which of the factors are used to gain access to user data after the TOE entered a Compliant power saving state. The TSS is inspected to ensure it describes that each authorization factor satisfies the requirements of FCS_AFA_EXT.1.1. The evaluator shall perform the following test: • Enter the TOE into a Compliant power saving state • Force the TOE to resume from a Compliant power saving state • Release an invalid authorization factor and verify that access to decrypted plaintext data is denied • Release a valid authorization factor and verify that access to decrypted plaintext data is granted.
Test Steps	• Cause the TOE to enter a compliant power saving state (i.e. Shutdown) • Cause the TOE to resume from a compliant power saving state • Enter incorrect authorization factors • Verify that access to the decrypted plaintext data is denied. • Enter correct authorization factors • Verify that access to the decrypted plaintext is granted.
Expected Test Results	• Cause the TOE to enter a compliant power saving state. (i.e Shutdown) • Cause the TOE to resume from a compliant power saving state. (the evaluator pressed the Power On button on the TOE)

	• Enter incorrect authorization factors and verify access to decrypted plaintext data is denied. ○ Note: The TOE does not display message such as “Invalid Credentials” or “Login Failed”. If an incorrect authorization factor is entered (i.e., in this case an incorrect password) the TOE simply clears the password field and presents the user with another password prompt. • Enter correct authorization factors • Access to the decrypted plaintext data is granted.
Pass/Fail with Explanation	Pass. The TOE only allows access to decrypted plaintext data once valid authorization factors have been presented.

6.1.3 FCS_CKM.1(b) [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR
Test Steps	There are no test evaluation activities for this SFR
Expected Test Results	There are no test evaluation activities for this SFR
Pass/Fail with Explanation	There are no test evaluation activities for this SFR

6.1.4 FCS_CKM.1(c) [EE]

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure the TOE to ensure the functionality of all selections.
Expected Test Results	The TOE should meet the functionality of all selections and it should not allow the user to configure the functionality.
Pass/Fail with Explanation	Pass. By default, the TOE meets the functionality of all selections and it does not allow the user to configure the functionality. This meets testing requirements.

6.1.5 FCS_CKM.4(a) [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR
Test Steps	There are no test evaluation activities for this SFR
Expected Test Results	There are no test evaluation activities for this SFR
Pass/Fail with Explanation	There are no test evaluation activities for this SFR

6.1.6 FCS_CKM.4(b) Test #1 [EE]

Item	Data
Test Assurance Activity	Test 1: Applied to each key held as plaintext in volatile memory and subject to destruction by overwrite by the TOE (whether or not the plaintext 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 shall: 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. 7. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails. Step 7 ensures that partial key fragments do not remain in memory. If a fragment is found, there is a miniscule chance that it is not within the context of a key (e.g., some random bits that happen to match). If this is the case the test should be repeated with a different key in Step #1. If a fragment is found the test fails.
Note 1	For Unlock Key- The Unlock key is immediately erased after user authentication has been attempted. Since changing the user passcode changes the Unlock key, and to meet the testing requirements, the vendor has proposed a novel solution where they could show the change of the existing Unlock key by having the user change their TOE user account passcode. To address this, the CCTL had submitted a TRRT Query Number 1096 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: “The Unlock Key is in volatile memory and the TOE can destroy that Unlock Key. The TRRT accepts that performing the AA as written in the SD will demonstrate that the SFR is satisfied.”
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: “The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied.”
Note 3	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 Coffee Lake 8557U and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Test Steps	• Record the initial value of the Unlock key. • Change the user account passcode. • Record the newer value of the Unlock key. • Search for the entire initial Unlock key value and verify that the key is not found.

	• Break the initial Unlock key value into similar sized pieces and verify that each piece of the key is not found. • Record the initial Ephemeral key value for System volume and Data volume on the TOE. • Reboot/shutdown the TOE. • Record the newer Ephemeral key value for System volume and Data volume on the TOE. • Search for the entire initial Ephemeral key values and verify that the keys are not found. • Break the initial Ephemeral key values into similar sized pieces and verify that each piece of the key is not found.
Expected Test Results	**Unlock Key:** The evaluator recorded the initial Unlock key value. Since the Unlock key changes by changing the user passcode, the evaluator changed the user password. The evaluator recorded the newer Unlock key value. After changing the user passcode, the evaluator then searched for the entire initial Unlock key and verified that the key was not found. The evaluator then searched for similar sized pieces and verified that the key was not found. This meets testing requirements. --- **Ephemeral Key:** The ephemeral key is randomly generated at each boot and destroyed at shutdown or reboot of the TOE platform. The evaluator recorded the initial Ephemeral key values for System volume and Data volume. • Record the initial Ephemeral Key for System Volume • Record the initial Ephemeral Key value for Data Volume 19G73 --- The evaluator then rebooted the TOE platform and recorded the newer Ephemeral key values for System volume and Data volume: • Record the changed Ephemeral Key for System Volume • Record the changed Ephemeral Key for Data Volume The evaluator searched for the entire initial System Volume Ephemeral Key and Data Volume Ephemeral Key and verified that the keys were not found. The evaluator then searched for similar sized pieces and verified that the keys were not found. This meets testing requirements
Pass/Fail with Explanation	Pass. The TOE successfully destroys the keys (i.e., Unlock key and Ephemeral key) from the TOE volatile memory. Furthermore, the evaluator was unable get a hit on the initial/original keys (i.e., neither the entire keys nor similar sized pieces of the keys). This meets the testing requirements.

6.1.7 FCS_CKM.4(b) Test #2 [EE]

Item	Data
Test Assurance Activity	Test 2: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location: 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 non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails. 5. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for test 1 above), and if a fragment is found in the repeated test then the test fails.
Note 1	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: “The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied.”
Test Steps	• Record the initial value of the Media key. • Perform a full erasure of the TOE platform (Detailed steps explained in Test Output) • Record the newer value of the Media key. • Search for the initial Media key value and verify that the key is not found. • Break the initial Media key value into similar sized pieces and verify that each piece of the key is not found. • Record the initial Volume Encryption key value for disk slice 6 (i.e., FV2) volume on the TOE. • Delete volume FV2. • Create a newer volume FV. • Record the newer Volume Encryption key value for disk slice 6 (i.e., FV) volume on the TOE. • Search for the entire initial Volume Encryption key value and verify that the key is not found. • Break the initial Volume Encryption key value into similar sized pieces and verify that each piece of the key is not found. • Record the Class A key for user 1 before logging into the TOE. • Verify the absence of the Class A key. • Login to the TOE as user 1. (i.e., represented by handle 501)

	• Record the Class A key value for user 1. (Note: According to vendor internal documents/mappings, Class A is numerically represented as Class 1) • Lock the TOE screen for user 1. • Dump the TOE memory contents and verify that Class A key for user 1 was destroyed. • Login to the TOE as user 1 and verify the presence of Class A key. • Lock the TOE screen and Login to the TOE as user 2 (i.e., represented by handle 502) • Record the Class A key value for user 2. (Note: According to vendor internal documents/mappings, Class A is numerically represented as Class 1) • Verify that Class A key for user 1 is destroyed but Class A key for user 2 is present. • Lock the TOE screen for both users and verify that the Class A key is destroyed for both the users.

Expected Test Results	**Media Key (mkey):**
	1. The **Media Key** (**mkey**) wraps the keying material, all metadata, and data on the FileVault protected volume. It is randomly generated when the volume is created/initialized. It is stored in encrypted format in non-volatile memory (Effaceable Storage)
	
	The evaluator recorded the Media Key (mkey) value.
	
	The media key (mkey) is erased after performing a full erasure of the TOE platform – this process is explained below:
	• Reboot the TOE into the Recovery OS:
	  ○ Restore from Time Machine Backup
	  ○ Reinstall macOS
	  ○ Get Help Online
	  ○ Disk Utility
	• The evaluator then opened the Terminal application on the TOE platform and typed #resetpassword command
	• Executing the resetpassword command triggers the launch of the Reset Password Application
	• The evaluator clicked on Recovery Assistant -> Erase Mac:
	• The evaluator then erased the TOE platform by clicking on “Erase Mac”
	• After the full erase takes place, the evaluator is placed back into the macOS Utilities window to select what process to use next.
	• The evaluator selected “Reinstall macOS” to complete the process. At this point, the SEP has erased and recreated the previous Media Key (mkey).
	• The new Media Key (mkey) was recorded as below: New-Media-key-After-ReInstall.txt
	• The evaluator searched for the entire original Media Key (mkey) and verified that the key was not found.
	• The evaluator then searched for similar sized pieces of the original Media key and verified that the Media key (mkey) was not found. This meets testing requirements.
	
	Volume Key:

	• The evaluator recorded the initial Volume Encryption Key value for disk slice 6 (i.e., Volume FV2 disk1s6) on the TOE platform. The Volume key is stored in encrypted format (wrapped with Class A KEK) in non-volatile memory. In the output below, Volume key is referred to as WVEK or Wrapped Volume Encryption Key. The evaluator executed the following command:fv1@FDE-TestMac ~ % apfsctl crypto -d disk1s6 • The evaluator then deleted the volume FV2 (disk1s6) from the TOE platform • The evaluator then created a newer volume named FV (i.e., disk1s6): • The evaluator then executed the following command and recorded the newer Volume Encryption Key: fv1@FDE-TestMac ~ % apfsctl crypto -d disk1s6 • The evaluator searched for the entire initial Volume Encryption Key and verified that the key was not found. • The evaluator then searched for similar sized pieces and verified that the key was not found. This meets testing requirements. --- **Class A Key:** Class A keys are only available while the host platform is unlocked and after the Unlock Key has been derived. • The evaluator recorded the contents of the non-volatile memory before the evaluator unlocked the TOE and verified that Class A key was absent: • The evaluator then logged in to the TOE as user 1 and recorded the contents of the non-volatile memory and verified the presence of the Class A key. (Note: According to the vendor's internal Class key mappings, Class A key is numerically represented by Class 1.) • The evaluator then Locked the TOE screen and recorded the contents of the non-volatile memory and verified that the Class A key for user 1 was destroyed. • The evaluator logged back into the TOE as user 1 and recorded the contents of the non-volatile memory and verified the presence of the Class A key. • The evaluator then locked the TOE screen for user 1 and then logged in to the TOE as a user 2. The evaluator verified that the Class A key for user 2 was present but Class A key for user 1 was absent. • The evaluator then locked the TOE screen for both the users and verified that Class A keys belonging to both the users were absent.
Pass/Fail with Explanation	Pass. The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory. Furthermore, the evaluator was unable get a hit on the initial/original keys (i.e., neither the entire keys nor similar sized pieces of the keys). This meets the testing requirements.

6.1.8 FCS_CKM.4(b) Test #3 [EE]

Item	Data
Test Assurance Activity	Test 3: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location: 1. Record the 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 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.
Note 1	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: "The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied."
Expected Test Results	• This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. • The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory. This meets the testing requirements.

6.1.9 FCS_CKM.4(d) Test #1 [AA + EE]

Item	Data
Test Assurance Activity	Test 1: Applied to each key held as plaintext in volatile memory and subject to destruction by overwrite by the TOE (whether or not the plaintext 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 shall: 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.

	7. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails. Step 7 ensures that partial key fragments do not remain in memory. If a fragment is found, there is a miniscule chance that it is not within the context of a key (e.g., some random bits that happen to match). If this is the case the test should be repeated with a different key in Step #1. If a fragment is found the test fails. 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 1. 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.
Note 1	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: “The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied.”
Expected Test Results	• This test is performed in conjunction with FCS_CKM.4(b) Test#1 [EE]. • The TOE successfully destroys the keys (i.e., Unlock key and Ephemeral key) from the TOE volatile memory. Furthermore, the evaluator should be unable to get a hit on the initial/original keys (i.e., neither the entire keys nor similar sized pieces of the keys).
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FCS_CKM.4(b) Test#1 [EE]. The TOE successfully destroys the keys (i.e., Unlock key and Ephemeral key) from the TOE volatile memory. Furthermore, the evaluator was unable get a hit on the initial/original keys (i.e., neither the entire keys nor similar sized pieces of the keys). This meets the testing requirements.

6.1.10 FCS_CKM.4(d) Test #2 [AA + EE]

Item	Data
Test Assurance Activity	Test 2: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall 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. 5. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for Use Case 1 test 1 above), and if a fragment is found in the repeated test then the test fails.
Note 1	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: “The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied.”
Expected Test Results	• This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. • The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory. This meets the testing requirements.

6.1.11 FCS_CKM.4(d) Test #3 [AA + EE]

Item	Data
Test Assurance Activity	Test 3: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall 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.

Note 1	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Note 2	The CCTL had submitted a TRRT Query Number 1095 to NIAP on 02/23/2021, and NIAP responded to the CCTL on 03/19/2021 with the following response: "The TRRT agrees that if the vendor testing harness (with the evaluators observing) can show that the key is destroyed, then the SFRs are satisfied."
Expected Test Results	• This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. • The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FCS_CKM.4(b) Test#2 [EE]. The TOE successfully destroys the keys (i.e., Media key, Volume key and Class A key) from the TOE non-volatile memory. This meets the testing requirements.

6.1.12 FCS_CKM_EXT.4(a) [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.13 FCS_CKM_EXT.4(b) [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.14 FCS_CKM_EXT.6 [EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.15 FCS_KDF_EXT.1 [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR
Test Steps	There are no test evaluation activities for this SFR
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR

6.1.16 FCS_KYC_EXT.1 [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR
Test Steps	There are no test evaluation activities for this SFR
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR

6.1.17 FCS_KYC_EXT.2 [EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR
Test Steps	There are no test evaluation activities for this SFR
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR

6.1.18 FCS_PCC_EXT.1 Test #1 [AA]

Item	Data
Test Assurance Activity	Test 1: Ensure that the TOE supports passwords/passphrases of a minimum length of 64 characters.
Test Steps	• Create a user account with a password of length 64 characters. • Verify the creation of the account is successful.
Expected Test Results	• Create a user account with a password of length 64 characters. • The creation of the account was successful as shown in the screenshot.
Pass/Fail with Explanation	Pass. The TOE supports a password length of 64 characters.

6.1.19 FCS_PCC_EXT.1 Test #2 [AA]

Item	Data
Test Assurance Activity	Test 2: If the TOE supports a password/passphrase length up to a maximum number of characters, n (which would be greater than 64), then ensure that the TOE will not accept more than n characters.
Test Steps	• Create a user account with a password of length 256 characters. • Verify the creation of the account is unsuccessful. • Create a user account with a password of length 255 characters. • Verify the creation of the account is successful.

Expected Test Results	• Create a user account with a password of length 256 characters. • The creation of the account is unsuccessful as the character count is greater than the supported 255 characters. The TOE did not allow the password of 256 characters to be entered in. • Create a user account with a password of length 255 characters. • The creation of the account is successful as the character count is maximum number of characters supported.
Pass/Fail with Explanation	Pass. The TOE supports a password length up to the specified amount listed in the ST.

6.1.20 FCS_PCC_EXT.1 Test #3 [AA]

Item	Data
Test Assurance Activity	Test 3: Ensure that the TOE supports passwords consisting of all characters assigned and supported by the ST author
Test Steps	• Create a user account with all the characters specified in the ST. • Verify the creation of the account is successful
Expected Test Results	• Create a user account with all the characters specified in the ST. • The creation of the account is successful as shown in the test output.
Pass/Fail with Explanation	Pass. The TOE supports passwords consisting of all characters specified in the ST.

6.1.21 FCS_SNI_EXT.1 [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.22 FCS_VAL_EXT.1 Test #1 [AA + EE]

Item	Data
Test Assurance Activity	Test 1: The evaluator shall determine the limit on the average rate of the number of consecutive failed authorization attempts. The evaluator will test the TOE by entering that number of incorrect authorization factors in consecutive attempts to access the protected data. If the limit mechanism includes any “lockout” period, the time period tested should include at least one such period. Then the evaluator will verify that the TOE behaves as described in the TSS.
Test Steps	• Configure the threshold (10) for failed attempts. • Attempt to authenticate User_3 for 10 times with an incorrect password as the authentication factor. • Verify that the TOE blocks the validation after 10 incorrect consecutive validation attempts.
Expected Test Results	• Configure the threshold value to 10 for failed attempts: • Attempt to authenticate the User_3 for 10 times with an incorrect password as the authentication factor and

	verify that the TOE blocks the validation after 10 consecutive validation attempts.
Pass/Fail with Explanation	Pass. The TOE does not allow access when the specified limit has been met.

6.1.23 FCS_VAL_EXT.1 Test #2 [AA]

Item	Data
Test Assurance Activity	Test 2: For each validated authorization factor, ensure that when the user provides an incorrect authorization factor, the TOE prevents the BEV from being forwarded outside the TOE (e.g., to the EE).
Note	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Test Steps	• Provide an incorrect authorization factor. • Verify the TOE prevents the BEV from being forwarded outside the TOE.
Expected Test Results	Note: According to the vendor naming convention, the Unlock key is referred to as the master_key. The Unlock key is the BEV. The evaluator provided an incorrect authorization factor (“test”) and observed that the TOE failed to authenticate the user. The Secure Enclave or SEP is a coprocessor fabricated within the system on chip (SoC) of the Apple T2 Security Chip, built solely to provide dedicated security functions. It protects the necessary cryptographic keys for FileVault.
Pass/Fail with Explanation	Pass. The TOE prevents the BEV from being forwarded when an incorrect authorization factor is provided.

6.1.24 FCS_VAL_EXT.1 Test #2 [EE]

Item	Data
Test Assurance Activity	Test 2: The evaluator shall force the TOE to enter a Compliant power saving state, attempt to resume it from this state, and verify that only a valid authorization factor as defined by the guidance documentation is sufficient to allow the TOE to exit the Compliant power saving state.

Test Steps	• For G2(S5)-Soft Off power saving state execute the following steps:
	  ○ For Password (Detailed steps are provided in the Test Output)
	  ▪ Force the TOE to enter a compliant power saving state.
	  ▪ When the TOE resumes, verify that only a valid authorization factor (Password) can resume the TOE’s activity.

Expected Test Results	**For G2(S5) – Soft Off and Password** • Force the TOE to enter a Compliant power saving state. • When the TOE resumes from this state, the TOE prompts the user for authorization factor (Password). • Before entering the password • After entering the password

	• Only valid authorization factors allow the TOE to resume from power saving state.
Pass/Fail with Explanation	Pass. Only valid authorization factors allow the TOE to exit the Compliant power saving state.

6.1.25 FDP_DSK_EXT.1 Test #1 [EE]

Item	Data
Test Assurance Activity	Test 1: Write data to random locations, perform required actions and compare: • Ensure TOE is initialized and, if hardware, encryption engine is ready; • Provision TOE to encrypt the storage device. For SW Encryption products, or hybrid products use a known key and the developer tools. • Determine a random character pattern of at least 64 KB; • Retrieve information on what the device TOE's lowest and highest logical address is for which encryption is enabled.
Test Steps	1. Enable FileVault 2. Open Disk Utility 3. Click Partition 4. Click + a. Set the Name to: "FDP_DSK_EXT1" b. Set the Format to: "Mac OS Extended (Journaled, Encrypted)" c. Set the Size to: 500 MB d. Click Apply 5. As root, write random bytes to the entire volume using "dd if=/dev/urandom of=/Volumes/FDP_DSK_EXT1/random conv=notrunc" The start of the file corresponds with the lowest logical address, and the end of the file corresponds with the highest logical address. 6. Determine the 3 random character patterns by running: a. head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin b. dd if=/Volumes/FDP_DSK_EXT1/random skip=512000 count=128 of=mid.bin # skip the first 512000x512 byte blocks ≈ 250 MB and copy 128x512 byte blocks = 64KB c. tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin
Expected Test Results	1. Enable FileVault 2. Open Disk Utility 3. Click Partition 4. Click + a. Set the Name to: "FDP_DSK_EXT1" b. Set the Format to: "Mac OS Extended (Journaled, Encrypted)" c. Set the Size to: 500 MB d. Click Apply Step 5: As root, write random bytes to the entire volume using "dd if=/dev/urandom of=/Volumes/FDP_DSK_EXT1/random conv=notrunc" The start of the file corresponds with the lowest logical address, and the end of the file corresponds with the highest logical address. Step 6: Determine the 3 random character patterns by running: a. head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin b. dd if=/Volumes/FDP_DSK_EXT1/random skip=512000 count=128 of=mid.bin # skip the first 512000x512 byte blocks ≈ 250 MB and copy 128x512 byte blocks = 64KB c. tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin

Pass/Fail with Explanation	Pass. The drive was encrypted, and a known random pattern was written to the lowest, highest, and middle logical addresses.

6.1.26 FDP_DSK_EXT.1 Test #2 [EE]

Item	Data
Test Assurance Activity	Test 2: Write pattern to storage device in multiple locations: • For HW Encryption, randomly select several logical address locations within the device's lowest to highest address range and write pattern to those addresses; • For SW Encryption, write the pattern using multiple files in multiple logical locations.
Test Steps	1. Determine the 3 random character patterns by running: - head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin - dd if=/Volumes/FDP_DSK_EXT1/random skip=512000 count=128 of=mid.bin # skip the first 512000x512 byte blocks ≈ 250 MB and copy 128x512 byte blocks = 64KB - tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin
Expected Test Results	1. Determine the 3 random character patterns by running: - head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin - dd if=/Volumes/FDP_DSK_EXT1/random skip=512000 count=128 of=mid.bin # skip the first 512000x512 byte blocks ≈ 250 MB and copy 128x512 byte blocks = 64KB - tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin -Record the pattern written to the lowest logical address. -Record the pattern written to the highest logical address. -Record the pattern written to the middle logical address.
Pass/Fail with Explanation	Pass. Random patterns were written to several addresses.

6.1.27 FDP_DSK_EXT.1 Test #3 [EE]

Item	Data

Test Assurance Activity	Test 3: Verify data is encrypted:
	• For HW Encryption:
	  ○ engage device's functionality for generating a new encryption key, thus performing an erase of the key per FCS_CKM.4(a);
	  ○ Read from the same locations at which the data was written;
	  ○ Compare the retrieved data to the written data and ensure they do not match
	• For SW Encryption, using developer tools;
	  ○ Review the encrypted storage device for the plaintext pattern at each location where the file was written and confirm plaintext pattern cannot be found.
	  ○ Using the known key, verify that each location where the file was written, the plaintext pattern can be correctly decrypted using the key.
	  ○ If available in the developer tools, verify there are no plaintext files present in the encrypted range.

Test Steps	1. Use Disk Utility to Erase the FDP_DSK_EXT1 partition 2. As root, execute the commands below: a. sudo dd if=/dev/urandom of=/Volumes/FDP_DSK_EXT1/random conv=notrunc b. head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin c. sudo dd if=/Volumes/FDP_DSK_EXT1/random of=mid.bin skip=512000 count=128 d. sudo dd if=/Volumes/FDP_DSK_EXT1/random of=mid.bin skip=102400 count=128 e. tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin f. sudo ./setsize /Volumes/FDP_DSK_EXT1/dump 131872384 3. Verity the patterns from FDP_DSK_EXT.1 Test #1 Step 6 do not appear: a. Perform the following conversions: i. xxd -p -c 128 start.bin > start.hex ii. xxd -p -c 128 mid.bin > mid.hex iii. xxd -p -c 128 end.bin > end.hex iv. xxd -p -c 256 dump.bin > dump.hex v. Note: The search patterns are broken into 128 character lines while the dump patterns are broken into 256 character lines, ensuring every other line in the search patterns would match, even if the exact starting byte offset for the dump differs from how the initial patterns were captured b. Perform a search using "./check-patterns.sh dump.hex start.hex mid.hex end.hex" i. This script searches dump.hex for each line contained in start.hex, mid.hex, and end.hex; and reports if any matches were found.
Expected Test Results	1. Use Disk Utility to Erase the FDP_DSK_EXT1 partition 1. Execute the commands below: sudo dd if=/dev/urandom of=/Volumes/FDP_DSK_EXT1/random conv=notrunc head -c 65536 /Volumes/FDP_DSK_EXT1/random > start.bin sudo dd if=/Volumes/FDP_DSK_EXT1/random of=mid.bin skip=512000 count=128 sudo dd if=/Volumes/FDP_DSK_EXT1/random of=mid.bin skip=102400 count=128 tail -c 65536 /Volumes/FDP_DSK_EXT1/random > end.bin ./setsize /Volumes/FDP_DSK_EXT1/dump 131872384 2. Copy the contents of the drive and check for patterns and Full check of all patterns. -The actual shell script and C program that were used to conduct this test are provided for reference.
Pass/Fail with Explanation	Pass. The patterns stored on the drive prior to the erase were not found on the drive after the erase.

6.1.28 FMT_MOF.1 Test #1 [AA]

Item	Data
Test Assurance Activity	Test 1: The evaluator presents a privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior and properties are allowed.
Test Steps	• Present privileged authorization credentials to the TOE. • Verify that changes can be made to the compliant power saving state behavior.

Expected Test Results	• Present privileged authorization credentials to the TOE.
	• Verify that changes can be made to the compliant power saving state behavior.
	  ○ Navigate to System Preferences->Energy Saver-> Schedule
	  ○ Enable and select Shutdown->Everyday->12:00AM.
	  ○ Click OK to save the changes.

Pass/Fail with Explanation	Pass. The TOE only allows users with privileged authorization credentials to make changes to the behavior of the compliant power saving state.

6.1.29 FMT_MOF.1 Test #2 [AA]

Item	Data
Test Assurance Activity	Test 2: The evaluator presents a non-privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior are not allowed.
Test Steps	• Login to the TOE as an unprivileged user (i.e., user_1). • Navigate to System Preferences->Energy Saver-> Schedule. • Attempt to make changes to the compliant power savings state (i.e., try to change the schedule). • Verify that the unprivileged user is unable to make changes to compliant power saving state.
Expected Test Results	• Login to the TOE as an unprivileged user (i.e., user_1) • Navigate to System Preferences->Energy Saver-> Schedule • Attempt to make changes to the compliant power savings state (i.e., try to change the schedule) ○ Note: All options in the figure below are greyed out which means that the unprivileged user is unable to make changes to the compliant power saving state. • Verify that the unprivileged user is unable to make changes to compliant power saving state. Note: The unprivileged user attempted to unlock the TOE, but the TOE prevented the user from making any changes to the TOE compliant power saving state.
Pass/Fail with Explanation	Pass. An un-privileged user is unable to modify the compliant power saving state behavior.

6.1.30 FMT_SMF.1(1) Test #1a/b [AA]

Item	Data
Test Assurance Activity	If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to forward a command to the EE to change and cryptographically erase the DEK. The actual testing of the cryptographic erase will take place in the EE.
Test Steps	1. Use Disk Utility to command the EE to change and cryptographically erase the DEK.

Expected Test Results	Step 1: Erase FDP_DSK_EXT1 Note: See FMT_SMF.1 Test #1a/b [EE] for the actual changing of the DEK.
Pass/Fail with Explanation	Pass. The TSF was able to send the EE a command to change and erase the DEK.

6.1.31 FMT_SMF.1 Test #1c [AA]

Item	Data
Test Assurance Activity	If item c) is selected in FMT_SMF.1.1: The evaluator shall initialize the TOE such that it requires the user to input an authorization factor in order to access encrypted data. Test 1: The evaluator shall first provision user authorization factors, and then verify all authorization values supported allow the user access to the encrypted data. Then the evaluator shall exercise the management functions to change a user's authorization factor values to a new one. Then he or she will verify that the TOE denies access to the user's encrypted data when he or she uses the old or original authorization factor values to gain access.
Test Steps	• Log into a user account using the appropriate authorization values. (i.e. acumen) • Verify the attempt is successful. • Change the user's authorization factor to new values. (i.e. acumen1234) • Verify the TOE denies access to the encrypted data when present with the old values. (i.e. acumen)
Expected Test Results	• Log into a user account using the appropriate authorization values. (i.e. acumen) • Verify the attempt is successful. • Change the user's authorization factor to new values. (i.e. acumen1234) • Verify the TOE denies access to the encrypted data when presented with the old values. (i.e. acumen)
Pass/Fail with Explanation	Pass. The TOE denies access to the encrypted data when presented with old authorization factor values.

6.1.32 FMT_SMF.1 Test #1d [AA]

Item	Data
Test Assurance Activity	If item d) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to initiate TOE firmware/software updates.
Test Steps	• Start macOS Safari, visit https://support.apple.com/downloads and then download macOS Catalina 10.15.7 Update. • Open the downloaded update and follow onscreen instructions. • Verify that the TOE has the functionality to initiate TOE firmware/Software updates.
Expected Test Results	Note: The current software version of TOE is macOS Catalina 10.15.7 • Start macOS Safari, visit https://support.apple.com/downloads and then download macOS Catalina 10.15.7 Update. • Open the downloaded update and follow onscreen instructions. Note: The TOE prompts the user to input the correct authorization factor (in this case password) before installing the TOE software/firmware update on the TOE. Note: The TOE provides the user the option to restart the TOE. After the user clicks on Restart, the TOE will automatically reboot and install the update. The actual installation and verification of the TOE firmware/software update is covered in FPT_TUD_EXT.1 Test #2 [AA +EE].

Pass/Fail with Explanation	Pass. The evaluator verified that the TOE has the functionality to initiate TOE firmware/software updates. This meets testing requirements.

6.1.33 FMT_SMF.1 Test #2 [AA]

Item	Data
Test Assurance Activity	If item e) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described. Test 2 (conditional): If the TOE provides default authorization factors, the evaluator shall change these factors in the course of taking ownership of the device as described in the operational guidance. The evaluator shall then confirm that the (old) authorization factors are no longer valid for data access.
Expected Test Results	The TOE does not provide default authorization factors. No additional management functions are claimed.
Pass/Fail with Explanation	Pass. The TOE does not provide default authorization factors. No additional management functions are claimed.

6.1.34 FMT_SMF.1 Test #3 [AA]

Item	Data
Test Assurance Activity	If item e) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described. Test 3 (conditional): If the TOE provides key recovery capability whose effects are visible at the TOE interface, then the evaluator shall devise a test that ensures that the key recovery capability has been or can be disabled following the guidance provided by the vendor.
Expected Test Results	The TOE does not provide key recovery capability. No additional management functions are claimed.
Pass/Fail with Explanation	Pass. The TOE does not provide key recovery capability. No additional management functions are claimed.

6.1.35 FMT_SMF.1 Test #4 [AA]

Item	Data
Test Assurance Activity	If item e) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described. Test 4 (conditional): If the TOE provides the ability to configure the power saving states that are entered by certain events, the evaluator shall devise a test that causes the TOE to enter a specific power saving state, configure the TSF so that this activity causes a different state to be entered, repeat the activity, and observe the new state is entered as configured.
Expected Test Results	The TOE does not provide the ability to configure the power saving state. No additional management functions are claimed.
Pass/Fail with Explanation	Pass. The TOE does not provide the ability to configure the power saving state. No additional management functions are claimed.

6.1.36 FMT_SMF.1 Test #5 [AA]

Item	Data
Test Assurance Activity	If item e) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described. Test 5 (conditional): If the TOE provides the ability to disable the use of one or more power saving states, the evaluator shall devise a test that enables all supported power saving states and demonstrates that the TOE can enter into each of these states. The evaluator shall then disable the supported power saving states one by one, repeating the same set of actions that were performed at the start of the test, and observe each time that when a power saving state is configured to no longer be used, none of the behavior causes the disabled state to be entered.
Expected Test Results	The TOE does not provide the ability to disable power saving state. No additional management functions are claimed.
Pass/Fail with Explanation	Pass. The TOE does not provide the ability to disable power saving state. No additional management functions are claimed.

6.1.37 FMT_SMF.1 Test #1a/b [EE]

Item	Data
Test Assurance Activity	If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to change and cryptographically erase the DEK (effectively removing the ability to retrieve previous user data).
Test Steps	1. Use Disk Utility to command the EE to change and cryptographically erase the DEK. 2. Verify the DEK was successfully changed.
Expected Test Results	Step 1: See FMT_SMF.1 Test #1a/b [AA] Step 2: Erase FDP_DSK_EXT1
Pass/Fail with Explanation	Pass. The TOE has the functionality to change and cryptographically erase the DEK.

6.1.38 FMT_SMF.1 Test #1c [EE]

Item	Data
Test Assurance Activity	If item c) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to initiate TOE firmware/software updates.
Expected Test Results	• This test is performed in conjunction with FMT_SMF.1 Test #1d [AA]. • TOE has the functionality to initiate TOE firmware/software updates.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FMT_SMF.1 Test #1d [AA]. The evaluator verified that the TOE has the functionality to initiate TOE firmware/software updates. This meets testing requirements.

6.1.39 FMT_SMF.1 Test #1d [EE]

Item	Data
Test Assurance Activity	If item d) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described.
Expected Test Results	No other functions have been selected and thus this test is not applicable.
Pass/Fail with Explanation	Pass. No other functions have been selected and thus this test is not applicable.

6.1.40 FMT_SMR.1 [AA]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.
Expected Test Results	There are no test evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

6.1.41 FPT_FAC_EXT.1 Test #1 [EE]

Item	Data
Test Assurance Activity	Test 1: The evaluator shall try installing a firmware upgrade and verify that a prompt is required and the appropriate value is necessary for the update to continue.
Expected Test Results	This test is performed in conjunction with FMT_SMF.1 Test #1d [AA]. The evaluator verified that the TOE prompts the user to enter the password for the admin account that is necessary for the update to continue.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FMT_SMF.1 Test #1d [AA]. The evaluator verified that the TOE prompts the user to enter the password for the admin account that is necessary for the update to continue.

6.1.42 FPT_FUA_EXT.1 Test #1 [EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.43 FPT_KYP_EXT.1 Test #1 [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

6.1.44 FPT_PWR_EXT.1 Test #1 [AA]

Item	Data
Test Assurance Activity	The evaluator shall confirm that for each listed compliant state all key/key materials are removed from volatile memory by using the test defined in FCS_CKM.4(d).
Note	The TOE runs on a Mac with the Apple T2 security chip. Since on a Mac with the Apple T2 chip, all FileVault key handling occurs in the Secure Enclave and that encryption keys are never directly exposed to the Intel CPU, there is no security relevance as to the Intel CPU used on the device. Since the Apple T2 Chip and the Intel CPU function independently, the various Intel micro-architectures are irrelevant to the protection of Data at Rest using FileVault. The testing was conducted on an Intel Core i7 8557U

	Coffee Lake and the same test evidence will be used across Intel Core i5 Coffee Lake 8500B and Intel Core i7 Ice Lake 1060NG7. This approach has been accepted by NIAP Validators during the synch meeting 02/19/2021.
Test Steps	• Record the initial Ephemeral key value for System volume and Data volume on the TOE. • Transition the TOE into compliant power savings state. • Transition the TOE out of the compliant power savings state. • Record the newer Ephemeral key value for System volume and Data volume on the TOE. • Search for the entire initial Ephemeral key values and verify that the keys are not found.
Expected Test Results	**Ephemeral Key:** The ephemeral key is randomly generated at each boot and destroyed at shutdown or reboot of the TOE platform. The evaluator recorded the initial Ephemeral key values for System volume and Data volume. • Record the value of the Ephemeral key before the TOE transitions into the compliant power savings state. • Record the initial Key for System Volume • Record Initial Ephemeral Key value for Data Volume 19G73 The evaluator transitioned the TOE into the compliant power savings state. The evaluator then verified that original Ephemeral key values were destroyed after the TOE transitioned out of the compliant power savings state. The evaluator recorded the newer Ephemeral key values for System volume and Data volume: • Record the changed Ephemeral Key for System Volume • Record the changed Ephemeral Key for Data Volume
Pass/Fail with Explanation	Pass. The evaluator confirmed that for each listed Compliant state (i.e. G2(S5)-Soft Off) all key/key materials were removed from volatile memory.

6.1.45 FPT_PWR_EXT.1 Test #1 [EE]

Item	Data
Test Assurance Activity	The evaluator shall confirm that for each listed Compliant state all key/key materials are removed from volatile memory by using the test indicated by the selection in FCS_CKM_EXT.6.
Expected Test Results	• This test is performed in conjunction with FPT_PWR_EXT.1 Test#1 [AA]. • For each listed Compliant state (i.e. G2(S5)-Soft Off) all key/key materials were removed from volatile memory.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FPT_PWR_EXT.1 Test#1 [AA]. The evaluator confirmed that for each listed Compliant state (i.e. G2(S5)-Soft Off) all key/key materials were removed from volatile memory.

6.1.46 FPT_PWR_EXT.2 Test #1 [AA]

Item	Data
Test Assurance Activity	The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a compliant power saving state by running the test identified in FCS_CKM.4(d).
Test Steps	• Click on Apple symbol and then click Shutdown • Verify that the TOE ends up in G2(S5)-Soft Off compliant power saving state.

Expected Test Results	• Click on Apple symbol and then click Shutdown • The evaluator then verified that the TOE shutdown after the evaluator initiated the Shutdown request.
Pass/Fail with Explanation	Pass. The TOE ends up in a compliant power savings state (G2(S5))- Soft Off.

6.1.47 FPT_PWR_EXT.2 Test #1 [EE]

Item	Data
Test Assurance Activity	The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a Compliant power saving state by using the test indicated by the selection in FCS_CKM_EXT.6.
Expected Test Results	• This test is performed in conjunction with FPT_PWR_EXT.2 Test#1 [AA]. • The TOE ends up in a compliant power savings state (G2(S5))- Soft Off.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FPT_PWR_EXT.2 Test#1 [AA]. TOE ends up in a compliant power savings state (G2(S5))- Soft Off.

6.1.48 FPT_TUD_EXT.1 Test #1 [AA + EE]

Item	Data
Test Assurance Activity	The evaluators shall perform the following tests (if the TOE supports multiple signatures, each using a different hash algorithm, then the evaluator performs tests for different combinations of authentic and unauthentic digital signatures and hashes, as well as for digital signature alone): Test 1: The evaluator performs the version verification activity to determine the current version of the TOE. After the update tests described in the following tests, the evaluator performs this activity again to verify that the version correctly corresponds to that of the update.
Test Steps	• Check the current version of the TOE by clicking on About this Mac • For actual installation of the TOE software/firmware update refer test FPT_TUD_EXT.1 Test #2 [AA+EE]. • After installing the TOE firmware/software update, verify that the version correctly corresponds to that of the update.
Expected Test Results	• Check the current version of the TOE by clicking on About this Mac. Note: The current software version of TOE is macOS Catalina 10.15.6. • For actual installation of the TOE software/firmware update refer test FPT_TUD_EXT.1 Test #2 [AA+EE]. • After installing the TOE firmware/software update, the evaluator verified that the newer version corresponds to that of the update- macOS Catalina 10.15.7.
Pass/Fail with Explanation	Pass. The TOE version correctly corresponds to that of the update.

6.1.49 FPT_TUD_EXT.1 Test #2 [AA + EE]

Item	Data
Test Assurance Activity	The evaluators shall perform the following tests (if the TOE supports multiple signatures, each using a different hash algorithm, then the evaluator performs tests for different combinations of authentic and unauthentic digital signatures and hashes, as well as for digital signature alone): Test 2: The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that an update successfully installs on the TOE. The

	evaluator shall perform a subset of other evaluation activity tests to demonstrate that the update functions as expected.
Test Bed	#1
Test Steps	• Check the current TOE firmware/software version. • Initiate and install the update on the TOE. • Verify that the update successfully installs on the TOE. • Perform subset of other evaluation activity such as changing the user password, checking the current TOE version to demonstrate that the update functions as expected.

Expected Test Results	• Check the current TOE firmware/software version
	  ○ Note: The current software version of TOE is macOS Catalina 10.15.6.
	• Start macOS Safari and visit https://support.apple.com/downloads. Then download macOS Catalina 10.15.7 Update
	• Open the downloaded update and follow onscreen instructions as shown.
	
	Note: The TOE prompts the user to input the correct authorization factor (in this case password) before installing the TOE software/firmware update on the TOE.
	
	Note: The TOE provides the user the option to restart the TOE. After the user clicks on Restart, the TOE will automatically reboot and install the update.
	• The evaluator verified that the TOE successfully installed the update as shown.
	• Perform subset of other evaluation activity such as changing the user password, checking the current TOE firmware/software version to demonstrate that the update functions as expected.
	  ○ Changing the user password for admin
	• Checking the current TOE firmware/software version

Pass/Fail with Explanation	Pass. The evaluator verified that an update successfully installs on the TOE. The evaluator performed a subset of other evaluation activities and verified that the update functions as expected. This meets the testing requirements.

6.1.50 FPT_TST_EXT.1 Test #1 [AA + EE]

Item	Data
Test Assurance Activity	There are no test evaluation activities for this SFR.
Test Steps	There are no test evaluation activities for this SFR.
Expected Test Results	There are no test evaluation activities for this SFR.
Pass/Fail with Explanation	There are no test evaluation activities for this SFR.

7 Security Assurance Requirements

7.1 ASE_CCL.1 Exact Conformance Actions

7.1.1 ASE_CCL.1

7.1.1.1 ASE_CCL.1.8 Activity 1

Objective	The evaluator shall check that the statements of security problem definition in the PP and ST are identical.
Evaluator Findings	The evaluator examined the section titled '**Security Problem Definition'** in the Security Target to verify that the statements of security problem definition in the PP and ST are identical. Upon investigation, the evaluator found that the Security Target states: **The security problem definition has been taken from [FDE EE v2.0e] and [FDE AA v2.0e] and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.** The evaluator found that the statements of security problem definition in the PP and ST are identical. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 ASE_CCL.1.9 Activity 1

Objective	The evaluator shall check that the statements of security objectives in the PP and ST are identical.
Evaluator Findings	The evaluator examined the section titled '**Security Objectives'** in the Security Target to verify that the statements of security objectives in the PP and ST are identical. Upon investigation, the evaluator found that the statements of security objectives in the PP and ST are identical. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.3 ASE_CCL.1.10 Activity 1

Objective	The evaluator shall check that the statements of security requirements in the ST include all the mandatory SFRs in the cPP, and all of the selection-based SFRs that are entailed by selections made in other SFRs (including any SFR iterations added in the ST). The evaluator shall check that if any other SFRs are present in the ST (apart from iterations of SFRs in the cPP) then these are taken only from the list of optional SFRs specified in the cPP (the cPP will not necessarily include optional SFRs, but may do so). If optional SFRs from the cPP are included in the ST then the evaluator shall check that any selection-based SFRs entailed by the optional SFRs adopted are also included in the ST.
Evaluator Findings	The evaluator examined the section titled '**Security Requirements'** in the Security Target verified that the statements of security requirements in the ST include all the mandatory SFRs in the cPP; all of the selection-based SFRs that are entailed by selections made in other SFRs (including any SFR iterations added in the ST); if any other SFRs are present in the ST then these are taken only from the list of optional SFRs specified in the cPP.

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

7.2 ADV_FSP.1 Basic Functional Specification

7.2.1 ADV_FSP.1

7.2.1.1 ADV_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.3 ADV_FSP.1 Activity 3

Objective	The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_OPE.1 Operational User Guidance

7.3.1 AGD_OPE.1

7.3.1.1 AGD_OPE.1 Activity 1

Objective	Operational guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.2 AGD_OPE.1 Activity 2

Objective	Operational guidance must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target. This may be contained all in one document.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are listed in table 1 “Table 1: Platforms”. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.3 AGD_OPE.1 Activity 3

Objective	In addition, the evaluator shall ensure that the following requirements are also met: • The operational guidance shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. 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 TOE. • The operational guidance shall describe how to configure the IT environments that are supported to shut down after an administratively defined period of inactivity. • The operational guidance shall identify system “sleeping” states for all supported operating environments and for each environment, provide administrative guidance on how to disable the sleep state. As stated above, the TOE developer may be providing an integrator’s guide and “power states” may be an abstraction that SEDs provide at various levels – e.g., may simply provide a command that the Host Platform issues to manage the state of the device, and the Host Platform is responsible for providing a more sophisticated power management scheme.

	• The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The operational guidance shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines. The section titled '**TOE Cryptographic Operation Hashing, Encryption and Decryption'** of the AGD was used to determine the verdict of this assurance activity. The evaluator verified the guidance documentation contains instructions to shut down after an administratively defined period of inactivity. The section titled '**Authorization Factors'** of the AGD was used to determine the verdict of this assurance activity. The evaluator verified the guidance documentation identifies system "sleeping" states for all supported operating environments and for each environment, provides administrative guidance on how to disable the sleep state. The section titled '**Authorization Factors**' of the AGD was used to determine the verdict of this assurance activity. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities. The entire AGD was used to determine the verdict of this assurance activity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 AGD_PRE.1 Preparative Procedures

7.4.1 AGD_PRE.1

7.4.1.1 AGD_PRE.1 Activity 1

Objective	Preparative procedures shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.3 AGD_PRE.1 Activity 2

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).
Evaluator Findings	The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the entire AGD. The evaluator found that these sections describe how the Operational Environment must meet: • Prerequisites for Installation • Installation of the Apple macOS Catalina 10.15 • TOE Cryptographic Operation Hashing, Encryption and Decryption • Creating User Accounts • Password Policy • Authorization Factors • Key Destruction • Validation of Cryptographic Elements • Enable Full Disk Encryption • TOE Startup Security Utility • TOE Self-Tests • Check Software Updates Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.4 AGD_PRE.1 Activity 3

Objective	Preparative procedures must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including the section titled '**TOE Description'** of AGD identifies the following supported platform are listed in table 1 "Table 1: Platforms". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.5 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment are listed and satisfied in the AGD_PRE.1 Activity 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.6 AGD_PRE.1 Activity 5

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Activity 4. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.1.7 AGD_PRE.1 Activity 6

Objective	In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must include instructions to provide a protected administrative capability.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability. The sections titled **'Creating User Accounts', 'Password Policy', 'Enable Full Disk Encryption, 'TOE Self-Tests' and 'TOE Startup Security Utility'** were used to determine the verdict of this work unit. The AGD describes configuring administration account changing password and implement security and encryption capabilities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5 ALC Assurance Activities

7.5.1 ALC_CMC.1

7.5.1.1 ALC_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5.2 ALC_CMS.1

7.5.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6 ATE_IND.1 Independent Testing – Conformance

7.6.1 ATE_IND.1

7.6.1.1 ATE_IND.1 Activity 1

Objective	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
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 the TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what is specified in the Security Target. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.3 ATE_IND.1 Activity 2

Objective	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.
Evaluator Findings	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. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.4 ATE_IND.1 Activity 3

Objective	The evaluator shall prepare a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must show in the test plan that each applicable testing requirement in the SFR-related Evaluation Activities is covered.
Evaluator Findings	The details of the testing of the TOE are found in the separate Test Reports and are summarized in chapter 6 of this document. The evaluator verified that all of the applicable SFR-related Evaluation Activities as well as all of the testing actions for ATE_IND.1 in the CEM are covered. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.5 ATE_IND.1 Activity 4

Objective	The test plan identifies the platforms to be tested, and for any 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.
Evaluator Findings	The details of the platforms tested are found in the separate Test Reports and are summarized in chapter 6 of this document. An analysis of the platforms included in the evaluation found in the separate Equivalency Analysis and are summarized in chapter 3 of this document. The evaluator verified that all platforms included in the evaluation are either tested or justification is provided for them being equivalent to a tested platform. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.7 ATE_IND.1 Activity 5

Objective	The test plan describes the composition and configuration of each platform to be tested, and any setup actions that are 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 any cryptographic engine to be used (e.g. for cryptographic protocols being evaluated).
Evaluator Findings	The details of the platform testbeds and configurations are found in the separate Test Reports and are summarized in chapter 4 of this document. The evaluator verified that the composition and configuration of each platform to be tested is documented. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.8 ATE_IND.1 Activity 6

Objective	The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives, and the expected results.
Evaluator Findings	The details of the testing of the TOE are found in the separate Test Reports and are summarized in chapter 6 of this document. The evaluator verified that high-level test objectives, test procedures, and expected results are provided for each test. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.9 ATE_IND.1 Activity 7

Objective	The test report (which could just be an updated 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, so that a fix was then installed and then a successful re-run of the test was carried out, then the report would show a “fail” result followed by a “pass” result (and the supporting details), and not just the “pass” result .
Evaluator Findings	The details of the testing of the TOE are found in the separate Test Reports and are summarized in chapter 6 of this document. The evaluator verified that actual results and verdicts are provided for each test. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.7 AVA_VAN.1 Vulnerability Survey

7.7.1 AVA_VAN.1

7.7.1.1 AVA_VAN.1 Activity 1

<table>
<tr><td>Objective</td><td>The evaluator formulates hypotheses in accordance with process defined in Appendix A.1. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.

Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

• http://cve.mitre.org/cve/
• http://nvd.nist.gov/
• http://www.kb.cert.org/vuls/html/search

The evaluator performed the public domain vulnerability searches using the following key words. The vulnerability search was performed on 04/20/2021.

The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include:

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

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

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

The table below presents items that were searched by CPE:
<table><tr><th>Component</th><th>CPE</th></tr><tr><td>Apple Mac Mini i5 8500B</td><td>cpe:2.3:h:apple:Mac:mini:*:*:*:*:macOS:i5-8500B:Macmini</td></tr></table></td></tr>
</table>

	Apple MacBook Air i7 1060NG-7	cpe:2.3:h:apple:MacBook:Air:*:*:*:*:macOS:i7-1060NG-7:MacBookAir
	Apple MacBookPro i7-8557U	cpe:2.3:h:apple:MacBook:Pro:*:*:*:*:macOS:i7-8557U:MacBookPro
	Apple sepOS 10.15.7	cpe:2.3:o:apple:sepOS:10.15.7:*:*:*:*:TxFW:Apple_T_Series:TxFW_4.7
	Apple sepOS 10.15.6	cpe:2.3:o:apple:sepOS:10.15.6:*:*:*:*:TxFW:Apple_T_Series:TxFW_4.6
	Apple T2 Security Chip	cpe:2.3:h:apple:Apple_Tx_Security_Chip:T2:*:*:*:*:TxFW:Apple_T2:iBridge
	Apple corecrypto kernel	cpe:2.3:*:apple:CoreCrypto_Kernel:10:10.15.7:*:*:*:macOS:x86_64:*
	Apple Secure Key Store sepOS	cpe:2.3:*:apple:Secure_Key_Store:10:10.15:*:*:TxFW:sepOS:Apple_T_Series:*
	The sources of the publicly available information are provided above. The evaluation lab examined each result provided from public databases to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. Based on these findings, this assurance activity is considered satisfied.	
Verdict	Pass	

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document