Cigent PBA Software v1.0.6

Assurance Activity Report

Version 0.12

October 2023

Document prepared by

Lightship Security

www.lightshipsec.com

Table of Contents

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security USA for the evaluation identified in Table 1. The AAR is produced in accordance with National Information Assurance Program (NIAP) reporting guidelines.

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Scheme	NIAP
Evaluation Facility	Lightship Security USA, Inc. 3600 O'Donnell Street, Suite 2 Baltimore, MD 21224
Developer/Sponsor	Cigent 2211 Widman Way, Suite 150 Fort Myers, Florida 33901
TOE	Cigent PBA Software v1.0.6
Security Target	Cigent PBA Software v1.0.6 Security Target, Version 2.5, October 2023
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition Version 2.0 + Errata 20190201 [PP]

1.2 Evaluation Methods

2 The evaluation was performed using the methods, tools and standards identified in Table 2.

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1 R5
Evaluation Methodology	CEM v3.1R5
Supporting Documents	Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition, February 2019, Version 2.0 + Errata 20190201 [SD]
Tools	See section 2.2.3

Table 3: Interpretations

TD #	Name	Source	Applicable?	Rationale
TD0458	FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities	CPP_FDE_AA	Yes	N/A
TD0606	FIT Technical Recommendation for Evaluating a NAS against the FDE AA and FDEE	CPP_FDE_AA	No	The TOE is not a NAS.
TD0759	FIT Technical Decision for FCS_AFA_EXT.1.1	CPP_FDE_AA	Yes	N/A
TD0760	FIT Technical Decision for FCS_SNI_EXT.1.3, FCS_COP.1(f)	CPP_FDE_AA	Yes	N/A
TD0764	FIT Technical Decision for FCS_PCC_EXT.1	CPP_FDE_AA	Yes	N/A
TD0765	FIT Technical Decision for FMT_MOF.1	CPP_FDE_AA	Yes	N/A
TD0766	FIT Technical Decision for FCS_CKM.4(d) Test Notes	CPP_FDE_AA	Yes	N/A
TD0767	FIT Technical Decision for FMT_SMF.1.1	CPP_FDE_AA	Yes	N/A
TD0769	FIT Technical Decision for FPT_KYP_EXT.1.1	CPP_FDE_AA	Yes	N/A

1.3 Reference Documents

Table 4: List of Reference Documents

Ref	Document
[PP]	Collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201
[SD]	Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition February 2019 Version 2.0 + Errata 20190201
[ST]	Cigent PBA Software v1.0.6 Security Target, Version 2.5, October 2023
[AGD]	Cigent PBA Software v1.0.6 Common Criteria Guide, Version 1.2, September 2023
[MAN]	Cigent PBA Installation Guide and User Manual, Aug 2023, V21
[KMD]	Cigent PBA Software v1.0.6 Key Management Description, Version 1.2, September 2023

Ref	Document
[ETR]	Cigent PBA Software v1.0.6 Evaluation Technical Report, Version 0.8, October 2023
[AAR]	Cigent PBA Software v1.0.6 Assurance Activity Report, Version 0.12, October 2023
[DTR]	Cigent PBA Software v1.0.6 cPP_FDE_AA Test Plan, Version 0.5, October 2023 Cigent PBA Software v1.0.6 cPP_FDE_AA Test Plan Evidence, Version 0.5, October 2023
[AVA]	Cigent PBA Software v1.0.6 Vulnerability Assessment, Version 0.3, October 2023

1.4 Summary of SFRs

Table 5: Summary of SFRs

Requirement	Title
FCS_AFA_EXT.1	Authorization Factor Acquisition
FCS_AFA_EXT.2	Timing of Authorization Factor Acquisition
FCS_CKM.4(a)	Cryptographic Key Destruction (Power Management)
FCS_CKM.4(d)	Cryptographic Key Destruction (Software TOE, 3rd Party Storage)
FCS_CKM_EXT.4(a)	Cryptographic Key and Key Material Destruction (Destruction Timing)
FCS_CKM_EXT.4(b)	Cryptographic Key and Key Material Destruction (Power Management)
FCS_KYC_EXT.1	Key Chaining (Initiator)
FCS_SNI_EXT.1	Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
FMT_MOF.1	Management of Functions Behavior
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_KYP_EXT.1	Protection of Key and Key Material
FPT_PWR_EXT.1	Power Saving States
FPT_PWR_EXT.2	Timing of Power Saving States
FPT_TUD_EXT.1	Trusted Update
Selection based	
FCS_CKM.1(b)	Cryptographic Key Generation (Symmetric Keys)

Requirement	Title
FCS_COP.1(a)	Cryptographic Operation (Signature Verification)
FCS_COP.1(b)	Cryptographic Operation (Hash Algorithm)
FCS_COP.1(c)	Cryptographic Operation (Keyed Hash Algorithm)
FCS_COP.1(g)	Cryptographic Operation (Key Encryption)
FCS_KDF_EXT.1	Cryptographic Key Derivation
FCS_PCC_EXT.1	Cryptographic Password Construct and Conditioning
FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
FCS_SMC_EXT.1	Submask Combining

2 TOE Details

2.1 Overview

3 The TOE is software that provides pre-boot authentication (PBA) for use with a self-encrypting drive (SED).

2.2 TOE Models/Platforms

4 The TOE is Cigent PBA Software v1.0.6.

2.2.1 Test Platform Equivalency

5 The [ST] claims a single TOE version (Cigent PBA Software v1.0.6). Full testing was performed on this software, thus no equivalency is considered.

2.2.2 TOE Test Configuration (testing environment)

6 The TOE is Cigent PBA Software v1.0.6. The evaluation fully tested this with the following non-TOE components:

1. **SED:** Cigent Secure SSD Advanced FIPS M.2 2280
2. **Protected OS:** Microsoft Windows 10
3. **Computer Hardware:** Dell Inspiron 15 with Intel Core i7-8550U
4. **Smartcard and reader:** Generic card reader with a FIPS 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcard.

2.2.3 Tools used in the test environment

Tool name	Version	Description
Cigent PBA Software 1.0.6.4 MEMTEST	1.0.6.4 MEMTEST	Instrumented TOE build to allow the evaluator to capture key values and offsets then dump memory to verify key destruction. This tool was used for FCS_CKM.4(d) testing only.
HxD	2.5.0.0	This tool was used to verify binary file dumps with key contents

3 Evaluation Activities for SFRs

3.1 Cryptographic Support (FCS)

3.1.1 FCS_AFA_EXT.1 Authorization Factor Acquisition

3.1.1.1 TSS

7 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.

Findings: Section 6.2.1 of the [ST] states that the TOE supports the use of password-only, smartcard-only and dual factor (username/password and smartcard) authentication. [AGD] Section 2.3 states that smart cards must be FIPS201 PIV-CAC compliant.

8 If other authorization factors are specified, then for each factor, the TSS specifies how the factors are input into the TOE.

Findings: The [ST] provides a detailed flow how the factors are input into the TOE. The authentication factors for the TOE comprise of:

<u>Password-Only Authentication Flow</u>

Section 6.2.1.1 describes password-only authentication as requiring the user to enter their username and password.

<u>Smartcard-Only Authentication Flow</u>

Section 6.2.1.2 describes smartcard-only authentication as requiring the user to present a smartcard and enter the smartcard PIN.

<u>Dual-Factor Authentication Flow</u>

Section 6.2.1.3 describes dual-factor authentication as comprising the input factors from both password authentication in the form of username and password followed by smartcard authentication which uses a smartcard and smartcard PIN.

3.1.1.2 Operational Guidance

9 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.

Findings: Section 2.3 of the [AGD] has a section labelled “Authorization Factors” lists the authorization factors that the TOE supports. This section states that Cigent PBA supports passwords, smart card and multi-factor authorization factors. Smart cards must be FIPS201 PIV-CAC compliant. This section references the appropriate sections of [MAN] which includes detailed instructions to configure each authorization factor.

3.1.1.3 KMD

10 The evaluator shall examine the Key Management Description to confirm that the initial authorization factors (submasks) directly contribute to the unwrapping of the BEV.

Findings:	The evaluator examined all keychains provided by the TOE in Figure 2, Figure 3 and Figure 4 of the [KMD]. All keychains listed are initiated with authentication factors (password-only, smartcard-only and dual factor) that contribute directly to unwrapping the BEV.

11 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).

Findings:	[KMD] Section 3.3 describes the Key Life-Cyle and included Table 3 which lists the derivation (submask) and strength of the keys.

3.1.1.4 Test

12 The password authorization factor is tested in FCS_PCC_EXT.1.

13 The evaluator shall also perform the following tests:

14 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.

High-Level Test Description
The evaluator attempted to log into the TOE independently with no password, no smartcard, correct password and no smartcard, and no password and correct smartcard and observed in each case that access to decrypted plaintext data was not granted.
Findings: PASS

3.1.2 FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition

3.1.2.1 TSS

15 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.

Findings:	[ST] Section 6.2.2 states that “Depending on the configuration, the user must authenticate via password-only, smartcard-only, or dual-factor to gain access to user data after the TOE enters a Compliant power saving state described by FPT_PWR_EXT.1." Section 6.2.1 also describes how each authorization factor complies with FCS_AFA_EXT.1.1.

3.1.2.2 Operational Guidance

16 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.

Findings:	[AGD] Section 2.5 states that "Successful authentication and authorization must be achieved using the authorization factors described in section 2.3 in order to resume access to protected data."

3.1.2.3 KMD

17 There are no KMD evaluation activities for this SFR.

3.1.2.4 Test

18 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.

High-Level Test Description
Note the TOE only supports the G3 Compliant power saving state. The evaluator attempted to log into the TOE independently with an invalid password, invalid smartcard, correct password and invalid smartcard, and invalid password and correct smartcard and observed in each case that access to decrypted plaintext data was not granted. The evaluator then attempted to log into the TOE independently with the correct password, correct smartcard, and correct password and correct smartcard (dual-factor) and observed in each case that access to decrypted plaintext data was granted.
Findings: PASS

3.1.3 FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)

3.1.3.1 TSS

19 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.

Findings:	Section 6.2.4 of the [ST] states that the TOE erases cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state with a single overwrite consisting of zeroes and ones as specified in FCS_CKM.4(d). Temporary keys are not tracked. The TSF (not the Operational Environment) is used to destroy keys from volatile memory.

3.1.3.2 Operational Guidance

20 The evaluator shall check the guidance documentation if the TOE depends on the Operational Environment for memory clearing and how that is achieved.

Findings: Section 6.2.4 of the [ST] states that the Operational Environment is not used to destroy keys. No additional guidance needed.

3.1.3.3 KMD

21 The evaluator shall check to ensure the KMD lists each type of key, its origin, possible memory locations in volatile memory.

Findings: Table 3 labelled "Key Life-Cycle" in section 3.3 of the [KMD] lists all keys, their origin (Derivation column) and location (Storage column).

3.1.3.4 Test

22 There are no test evaluation activities for this SFR.

3.1.4 FCS_CKM.4(d) Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (TD0766)

Technical Decision: The evaluation activities were modified per TD0766.

3.1.4.1 TSS + KMD (Key Management Description may be used if necessary details describe proprietary information)

23 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.

Findings: [ST] Section 6.2.5 references the [KMD] regarding the details of how keys are managed in volatile memory. [KMD] "Table 3: Key Life-Cycle" outlines how each identified key is introduced into volatile memory under the "Derivation" column. Overwrite information for these keys is located under "End-of_life/When key is destroyed" column of the same table.

24 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).

Findings: [ST] Section 6.2.4 states that the TOE forwards a request to the EE to erase the DEK by uninstalling or erasing the entire disk. The Opal Revert Tper command is sent to the drive which is immediately followed by a crypto erase. [KMD] Section 3.2 reiterates the statement in [ST] section 6.2.4. [KMD] Table 3 also lists how the TOE derived, protects, stores, and destroys each key.

25 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.

Findings: [KMD] Section 3.2 addresses the key destruction for both volatile and non-volatile memory. [KMD] Table 3 also lists how the TOE derived, protects, stores, and destroys each key. This supports the [ST] claims for FCS_CKM.4(d) and the (TSS) section 6.2.5.

26 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.

Findings: [ST] Section 6.2.5 states that a single overwrite of zeroes and ones is used for key destruction in volatile memory. This supports the FCS_CKM.4(d) claims. Section 6.2.5 also describes the use of the Opal Revert Tper command to destroy keys from non-volatile memory which also supports the FCS_CKM.4(d) claim. No configurations or circumstances are identified which the TOE does not strictly conform to the key destruction requirement.

3.1.4.2 Operational Guidance

27 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.

Findings: [AGD] Section 2.4 labelled “Cryptographic Key Destruction” states that there are no situations where key destruction would be delayed or prevented.

28 For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, it is assumed the drive supports the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

Findings: [AGD] Section 2.4 labelled “Cryptographic Key Destruction” states that there are no situations where key destruction would be delayed or prevented.

29 Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. It is assumed the operating system and file system of the OE support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion.

Findings: [AGD] Section 2.4 labelled “Cryptographic Key Destruction” states that there are no situations where key destruction would be delayed or prevented.

30 It is assumed that if a RAID array is being used, only set-ups that support TRIM are utilized. It is assumed if the drive is connected via PCI-Express, the operating system supports TRIM over that channel. It is assumed the drive is healthy and contains minimal corrupted data and will be end of life before a significant amount of damage to drive health occurs, it is assumed there is a risk small amounts of potentially recoverable data may remain in damaged areas of the drive.

Findings:	No RAID array set ups are being used by the TOE, therefore this activity is not applicable.

31 Finally, it is assumed the keys are not stored using a method that would be inaccessible to TRIM, such as being contained in a file less than 982 bytes which would be completely contained in the master file table.

Findings:	[AGD] Section 2.4 labelled “Cryptographic Key Destruction” states that there are no situations where key destruction would be delayed or prevented.

3.1.4.3 Tests

32 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.

33 Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

34 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.

High-Level Test Description
The evaluator created a new admin user in the system and set up a password and a smartcard. The evaluator then performed actions on the TOE so that the key was destroyed. The evaluator then dumped the content of the memory, searched for the key value, the key value broken into thirds and its offset and looked for the key inside the memory dump and confirmed it was removed from the memory. This was repeated for all keys and keychains.
Findings: PASS

35 The following tests apply only for the selection of “logically addresses the storage location…” 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). For the selection of “instructs the underlying platform…”, 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.

36 For the selection of “logically addresses the storage location…”, the following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern.

37 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.

High-Level Test Description
The above test is not applicable since the ST claims that it destroys the abstraction which represents the key.
Findings: N/A

38 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.

39 The test succeeds if correct pattern is used to overwrite the key in the memory location.

40 If the pattern is not found the test fails.

High-Level Test Description
The above test is not applicable since the ST claims that it destroys the abstraction which represents the key.

High-Level Test Description
Findings: N/A

3.1.5 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)

3.1.5.1 TSS

41 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 they should be expected to be destroyed.

Findings:	Section 6.2.6 of the [ST] states that keys are no longer needed when power is removed from memory, when the TOE erases the disk, or when the TOE is uninstalled. All intermediate keys are destroyed after their use in the chain. For example, for password-only authentication, SUB1 is destroyed subsequent to the decryption of the AK. Additional details regarding timing of key destruction are provided in the [KMD].

3.1.5.2 Operational Guidance

42 There are no AGD evaluation activities for this SFR.

3.1.5.3 KMD

43 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.

Findings:	The [KMD] provides “Table 3: Key Life-Cycle” which describes all keys, their storage location (Storage column) and destruction events (End-of-life / When key is destroyed column).

44 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.

Findings:	[KMD] Table 3 “Key Life-Cycle” contains the location of keys and key material under the column labelled “Storage, it’s use is found under the column labelled “Purpose” and its destruction method is under the column labelled “End-of-life/When key is destroyed”. [KMD] Section 3.2 discusses key destruction for power-saving states. Keys are destroyed by the time the SED is unlocked (which is prior to entering a power saving state) and are re-introduced to RAM when unlocking the SED after entering a power saving state (re-authentication to the TOE is required). This is consistent with FCS_CKM.4(a).

3.1.5.4 Test

45 There are no test evaluation activities for this SFR.

3.1.6 FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)

3.1.6.1 TSS

46 The evaluator shall verify the TSS provides a description of what keys and key material are destroyed when entering any Compliant power saving state.

Findings:	[ST] Section 6.2.7 states that all keys and keying material are destroyed when transitioning to a compliant power saving state.

3.1.6.2 Operational Guidance

47 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.

Findings:	[AGD] Section 2.5 states that an unexpected power loss would result in the G3 power state. To resume use of the TOE, users will be required to re-authenticate.

3.1.6.3 KMD

48 The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.

Findings:	Table 3 of the [KMD] lists keys under the column labelled “Key/CSP” which can be mapped to the storage location under the column labelled “Storage.”

49 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.

Findings:	[KMD] Table 3 “Key Life-Cycle” contains the location of keys and key material under the column labelled “Storage, it’s use is found under the column labelled “Purpose” and its destruction method is under the column labelled “End-of-life/When key is destroyed”. [KMD] Section 3.2 discusses key destruction for both volatile and non-volatile memory. Keys in volatile memory are destroyed by a single overwrite consisting of zeroes and ones. Keys in non-volatile memory are destroyed using the Opal Revery Tper command. Both of these descriptions are consistent with the FCS_CKM.4(d) claims in [ST].

3.1.6.4 Test

50 There are no test evaluation activities for this SFR.

3.1.7 FCS_KYC_EXT.1 Key Chaining (Initiator)

3.1.7.1 TSS

51 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 AES-128, and no fewer than 256 bits for products that support AES-256.

Findings:	[ST] Section 6.2.13 states that the TOE supports BEV (AK) sizes of 256 bits. Additional details on the TOE key chain are provided in section 6.1.2. The keychain Figures 1, 2 and 3 in section 6.1.2 indicate that the BEV size of 256 bits matches the claimed AES key size (256 bits).

3.1.7.2 Operational Guidance

52 There are no AGD evaluation activities for this SFR.

3.1.7.3 KMD

53 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.

Findings:	The evaluator examined all keychains provided by the TOE in Figure 2, Figure 3 and Figure 4 of the [KMD]. All keychains listed are initiated with authentication factors (password-only, smartcard-only and dual factor) that contribute directly to unwrapping the BEV. The key derivation functions in these figures are consistent with FCS_KDF_EXT.1. FCS_COP.1(d) is not selected by the [ST]

54 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.

Findings:	[KMD] Section 3.1 provides Figure 2, Figure 3 and Figure 4 which depicts the keychain process for each authorization method. Section 3.1.3 describes the process to derive keys in detail. The evaluator inspected this process to conclude that the key chain does not expose material that might compromise the key chain and the key chain could not be broken without the initial authorization value or cryptographic exhaust.

55 The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

Findings:	[KMD] Section 3.1 provides Figure 2, Figure 3 and Figure 4 which depicts the keychain for each authorization method. Each keychain uses 256-bit keys throughout the chain which is sufficient to protect the 256-bit BEV.

3.1.7.4 Test

56 There are no test evaluation activities for this SFR.

3.1.8 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (TD0760)

Technical Decision: The evaluation activities were modified per TD0760.

3.1.8.1 TSS

57 If salts are used, 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.

Findings:	Section 6.2.17 of the [ST] states that salts are generated using the RBG as described in FCS_RBG_EXT.1. Further details of FCS_RBG_EXT.1 is located in section 6.2.15 of the TSS.

58 If IVs or nonces are used, 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.

Findings:	Section 6.2.17 of the [ST] states that the TOE does not make use of nonces. IVs are generated by using the RBG as described in FCS_RBG_EXT.1. Tweaks are not considered since the [ST] does not claim an AES mode that utilizes tweaks.

3.1.8.2 Operational Guidance

59 There are no AGD evaluation activities for this SFR.

3.1.8.3 KMD

60 There are no KMD evaluation activities for this SFR.

3.1.8.4 Test

61 There are no test evaluation activities for this SFR.

3.2 Security management (FMT)

62 The evaluator shall perform the following test for each method of local login allowed:

3.2.1 FMT_MOF.1 Management of Functions Behavior (TD0765)

Technical Decision: The evaluation activities were modified per TD0765.

3.2.1.1 TSS

63 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.

Findings:	[ST] Section 6.3.1 states that the TOE does not allow any modification related to power saving states.

3.2.1.2 Operational Guidance

64 The evaluator to check if guidance documentation describes which authorization factors are required to change Compliant power saving state behavior and properties.

Findings: The TOE does not allow modification related to power saving states. [ST] Section 6.3.1 states that the TOE does not allow any modification related to power saving states.

3.2.1.3 KMD

65 There are no KMD evaluation activities for this SFR.

3.2.1.4 Test

66 The evaluator shall perform the following tests:

67 Test 1 (conditional): If the product supports changes to complaint power saving states, the evaluator presents a privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior and properties are allowed.

High-Level Test Description
The TOE does not allow any modification related to power saving states.
Findings: N/A

68 Test 2 (conditional): If the product supports changes to the compliant power saving states, the evaluator presents a non-privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior are not allowed.

High-Level Test Description
The TOE does not allow any modification related to power saving states.
Findings: N/A

3.2.2 FMT_SMF.1 Specification of Management Functions (TD0767)

Technical Decision: The evaluation activities were modified per TD0767.

3.2.2.1 TSS

69 If item a) 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.

Findings: Section 6.3.2 of the [ST] states that the TOE GUI may be used to forward requests to cryptographically erase the DEK to the EE via the GUI by uninstalling the TOE or erasing the entire disk. Changing the DEK is the same functionally as cryptographically erasing the DEK.

70 If item b) 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.

Findings: Section 6.3.2 of the [ST] states that the TOE GUI may be used to forward requests to cryptographically erase the DEK to the EE via the GUI by uninstalling the TOE or erasing the entire disk. On the admin's request, the Opal Revert Tper command is sent to the drive followed immediately by a crypto erase (format nvm).

71 If item c) 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.

Findings: Section 6.3.2 of the [ST] states that the TOE GUI may be used by the user to configure the authorization factors (password-only, smartcard-only, and password + smartcard).

72 If item d) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.

Findings: Section 6.3.2 of the [ST] states that the TOE updates may be performed by booting the host system with a USB drive that contains the PBA OS, utility, and the updated PBA content. An admin user must authenticate and choose to install the update.

73 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.

Findings: [ST] does not make any additional selections for e).

3.2.2.2 Operational Guidance

74 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.

Findings: [AGD] Section 2.6 "Management Functions" points to [MAN] for instructions on how to request changes to the DEK and cryptographic erasure of the DEK. These can be found under "Uninstall PBA" and "Erase Entire Disk" of [MAN].

75 If item c) 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.

Findings: [AGD] Section 2.6 "Management Functions" points to [MAN] for instructions on how to change authorization factors. These can be found under "Add User", "Edit User" and "Settings > Require Two-Factor Authentication" of [MAN].

76 If item d) 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.

Findings: [AGD] Section 2.7 "Updating Cigent PBA" provides the instruction for the admin on how to update the TOE. This includes updates performed by booting the host system with a USB drive containing the updated PBA content. The admin must then authenticate and choose to install the update provided by the USB drive. Section 2.7 refers to [MAN] section 6 for specific instructions to update the TOE.

77 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.

Findings:	[ST] does not make any additional selections for e).

78 Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.

Findings:	[ST] does not make this selection for e).

79 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).

Findings:	[AGD] Section 2.5 states that users interact with the protected OS or hardware platform to enter the claimed power state. Users are instructed to refer to the protected OS guidance to trigger a transition in power state.

3.2.2.3 KMD

80 There are no KMD evaluation activities for this SFR.

3.2.2.4 Test

81 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.

High-Level Test Description
The evaluator uninstalled the TOE and then reinstalled it to change the DEK. The evaluator then performed a cryptographic erase of the DEK and confirmed that the protected OS does not load.
Findings: PASS

82 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.

83 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.

High-Level Test Description
FCS_AFA_EXT.2 shows all authorization values allow the user to access encrypted data. The evaluator changed each authorization factor and confirmed that the TOE denies access to the encrypted data when the old authorization factor is used.
Findings: PASS

84 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.93 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.

High-Level Test Description
The evaluator performed this test in conjunction with FPT_TUD_EXT.1 Test 2.
Findings: PASS

85 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.

High-Level Test Description
Test not applicable. The ST does not claim additional functions for item e).
Findings: N/A

86 Test 2 (conditional): If the TOE provides default authorization values, the evaluator shall change these values in the course of taking ownership of the device as described in the operational guidance. The evaluator shall then confirm that the (old) authorization values are no longer valid for data access.

High-Level Test Description
Test not applicable. The TOE does not provide default authorization values. The authorization values are set during TOE set up.
Findings: N/A

87 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.

High-Level Test Description
Test not applicable. The TOE does not provide the key recovery capability.
Findings: N/A

88 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.

High-Level Test Description
Test not applicable. The TOE does not provide the ability to configure the power saving state.
Findings: N/A

89 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.

High-Level Test Description
Test not applicable. The TOE does not provide the ability to disable the power saving state.
Findings: N/A

3.2.3 FMT_SMR.1 Security Roles

3.2.3.1 TSS

90 There are no TSS evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

3.2.3.2 Operational Guidance

91 There are no guidance evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

3.2.3.3 KMD

92 There are no KMD evaluation activities for this SFR.

3.2.3.4 Test

93 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.

3.3 Protection of the TSF (FPT)

3.3.1 FPT_KYP_EXT.1 Protection of Key and Key Material (TD0458)

Technical Decision: The evaluation activities were modified per TD0458.

3.3.1.1 TSS

The evaluator shall examine the TSS and verify it identifies the methods used to protect keys stored in non-volatile memory.

Findings:	[ST] Section 6.4.1 states that the AK is encrypted per FCS_COP.1(g) in the TOE's database (non-volatile memory).

3.3.1.2 Operational Guidance

94 There are no AGD evaluation activities for this SFR.

3.3.1.3 KMD

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.

Findings:	[KMD] Section 3 all of the information for this activity. Figures 2, 3 and 4 as well as Table 3 describe the key chain in detail. All keys are encrypted per FCS_COP.1(g) in non-volatile memory.

3.3.1.4 Test

95 There are no test evaluation activities for this SFR.

3.3.2 FPT_PWR_EXT.1 Power Saving States

3.3.2.1 TSS

96 The evaluator shall validate the TSS contains a list of Compliant power saving states.

Findings:	[ST] Section 6.4.2 states that the TOE supports the G3 Compliant power saving state. This is consistent with the FPT_PWR_EXT.1 SFR claims.

3.3.2.2 Operational Guidance

97 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.

Findings:	[AGD] Section 2.1 notes that compliant power states supported by the Cigent PBA are described in section 2.5. Section 2.5 “Power Saving States” lists G3 as the only compliant power saving state. No additional guidance for disabling other power saving states is required.

3.3.2.3 KMD

98 There are no KMD evaluation activities for this SFR.

3.3.2.4 Test

99 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).

High-Level Test Description
The evaluator performed this test in conjunction with FCS_CKM.4(d). The TOE only supports powered on and powered off mode. Keys were confirmed to be destroyed when powered on. By definition, volatile memory is cleared in the powered off state.
Findings: PASS

3.3.3 FPT_PWR_EXT.2 Timing of Power Saving States

3.3.3.1 TSS

100 The evaluator shall validate that the TSS contains a list of conditions under which the TOE enters a Compliant power saving state.

Findings:	[ST] Section 6.4.3 states that the TOE enters a Compliant power saving states as prompted by the protected OS and user-initiated requests.

3.3.3.2 Operational Guidance

101 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.

Findings:	[AGD] Section 2.5 “Power Saving States” states that the TOE is in the G3 power saving state when the system is completely off and is not consuming any power. In the event of an unexpected power loss, the TOE will also enter the G3 state.

3.3.3.3 KMD

102 There are no KMD evaluation activities for this SFR.

3.3.3.4 Test

103 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).

High-Level Test Description
The evaluator performed this test in conjunction with FCS_CKM.4(d). The TOE only supports powered on and powered off mode. Keys were confirmed to be destroyed when powered on. By definition, volatile memory is cleared in the powered off state.
Findings: PASS

3.3.4 FPT_TUD_EXT.1 Trusted Update

3.3.4.1 TSS

104 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.

Findings:	[ST] Section 6.4.4 states that update filed are digitally signed (RSA per FCS_COP.1(a)) by Cigent and verified by the TOE before installation. Only authorized administrators may manually perform updates.

105 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.

Findings:	[ST] Section 6.4.4 states that update is verified by the TOE.

3.3.4.2 Operational Guidance

106 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.

Findings:	[AGD] Section 2.7 “Updating Cigent PBA” describes that the TOE is updated manually by an admin using a USB drive that contains the PBA OS, utility and updated PBA content. These update files are digitally signed by Cigent and verified by the TOE prior to installation. If the signature verification is successful, then the TOE boots as normal. In the case that a signature verification fails then the update is aborted, and an error message will be displayed which reads “Failed to load Pre-Boot. Validation failed.”

3.3.4.3 KMD

107 There are no KMD evaluation activities for this SFR.

3.3.4.4 Test

108 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):

109 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.

High-Level Test Description
The evaluator performed this test in conjunction with FPT_TUD_EXT.1 Test 2.
Findings: PASS

110 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.

High-Level Test Description
The evaluator verified the initial version of the TOE, initiated an update and at the end checked that the new version matched the expected version from the update. After that, the evaluator performed again the tests done in FCS_AFA_EXT.2 and FMT_SMF.1 Test 1 on the updated TOE version.
Findings: PASS

4 Evaluation Activities for Optional Requirements

No optional requirements are selected for this evaluation.

5 Evaluation Activities for Selection-Based Requirements

5.1 Cryptographic Support (FCS)

5.1.1 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)

111 TSS

112 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.

Findings:	[ST] Section 6.2.3 states that the TOE generates 256-bit AES keys for the AK (BEV). Depending on the configuration, the BEV is protected by the authentication factors described in section 6.2.1 of the TSS.

5.1.1.1 Operational Guidance

113 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.

Findings:	[ST] makes a single selection for 256-bit keys. [AGD] Section 2.2 “Configuration” states that “There are no specific steps required to establish the evaluated configuration.” The key size claimed is supported by the TOE by default.

5.1.1.2 KMD

114 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.

Findings:	[KMD] Section 3.1 “Keychains” provides Figure 2, 3 and 4 which shows the keychain for all methods of authentication. The 256-bit symmetric keys are used to encrypt the BEV using AES-256-GCM.

5.1.1.3 Test

115 There are no test evaluation activities for this SFR.

5.1.2 FCS_COP.1(a) Cryptographic Operation (Signature Verification)

116 This requirement is used to verify digital signatures attached to updates from the TOE manufacturer before installing those updates on the TOE. Because this component is to be used in the update function, additional Evaluation Activities to those listed below are covered in other evaluation activities sections in this document. The following activities deal only with the implementation for the digital signature algorithm; the evaluator performs the testing appropriate for the algorithm(s) selected in the component.

117 Hash functions and/or random number generation required by these algorithms must be specified in the ST; therefore the Evaluation Activities associated with those functions are contained in the associated Cryptographic Hashing and Random Bit Generation sections. Additionally, the only function required by the TOE is the

verification of digital signatures. If the TOE generates digital signatures to support the implementation of any functionality required by this cPP, then the applicable valuation and validation scheme must be consulted to determine the required evaluation activities.

5.1.2.1 TSS

118 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).

Findings: [ST] Section 6.2.8 states that the TOE performs signature verification using RSA 4096 with SHA-512 for trusted updates as follows:

a) TOE updates are signed with the Cigent code signing private key

b) The obfuscated public key is embedded in the TOE binary

c) When the user triggers the TOE update from the GUI, the TOE verifies the digital signature using the embedded public key

d) If the digital signature verification succeeds, the upgrade process is carried out

e) If the digital signature verification fails, the upgrade process is aborted, and an error is displayed to the user.

No additional processing is performed.

5.1.2.2 Operational Guidance

119 There are no AGD evaluation activities for this SFR.

5.1.2.3 KMD

120 There are no KMD evaluation activities for this SFR.

5.1.2.4 Test

121 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.

122 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.

123 The following tests are conditional based upon the selections made within the SFR.

124 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.

125 **ECDSA Algorithm Tests**

126 **ECDSA FIPS 186-4 Signature Verification Test**

127 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.

128 **RSA Signature Algorithm Tests**

129 **Signature Verification Test**

130 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.

131 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.

Findings: The vendor uses the CAVP certificate A4388 for RSA (4096-bit) signature verification per FIPS PUB 186-4. This is described in [ST] Table 4.

5.1.3 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)

5.1.3.1 TSS

132 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.

Findings: [ST] Section 6.2.9 states that the TOE makes use of SHA-512 for digital signature verification and PBKDF. The TOE also makes use of SHA-256 for submask combining.

5.1.3.2 Operational Guidance

133 The evaluator checks the operational guidance documents to determine that any system configuration necessary to enable required hash size functionality is provided.

Findings: The TOE uses the hash algorithms by default to the functions identified in the TSS activity above. [AGD] Section 2.2 "Configuration" states that "There are no specific steps required to establish the evaluated configuration."

5.1.3.3 KMD

134 There are no KMD evaluation activities for this SFR.

5.1.3.4 Test

135 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.

136 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.

137 **Short Messages Test Bit-oriented Mode**

138 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.

139 **Short Messages Test Byte-oriented Mode**

140 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.

141 **Selected Long Messages Test Bit-oriented Mode**

142 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.

143 **Selected Long Messages Test Byte-oriented Mode**

144 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.

145 **Pseudorandomly Generated Messages Test**

146 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.

Findings:	The vendor uses the CAVP certificate A4388 for SHA-256 and SHA-512 hashing per ISO/IEC 10118-3:2004. This is described in [ST] Table 4.

5.1.4 FCS_COP.1(c) Cryptographic Operation (Keyed Hash Algorithm)

5.1.4.1 TSS

147 If HMAC was selected:

148 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.

Findings:	[ST] Section 6.2.10 states that the TOE implements HMAC-SHA-512 with: Key length of 512 bits, Block size of 1024 bits, and MAC length of 512 bits.

149 If CMAC was selected:

150 The evaluator shall examine the TSS to ensure that it specifies the following values used by the CMAC function: key length, block cipher used, block size (of the cipher), and output MAC length used.

Findings:	[ST] Does not select CMAC.

5.1.4.2 Operational Guidance

151 There are no AGD evaluation activities for this SFR.

5.1.4.3 KMD

152 There are no KMD evaluation activities for this SFR.

5.1.4.4 Test

153 If HMAC was selected:

154 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.

Findings:	The vendor uses CAVP certificate A4388 for HMAC-SHA-512 message authentication with key size 256 bits per ISO/IEC 9797-2:2011. This is described in [ST] Table 4.

155 If CMAC was selected:

156 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.

Findings: [ST] Does not select CMAC.

5.1.5 FCS_COP.1(g) Cryptographic Operation (Key Encryption)

5.1.5.1 TSS

157 The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for the key encryption.

Findings: [ST] Section 6.2.11 states that the TOE performs key encryption using AES-GCM-256.

5.1.5.2 Operational Guidance

158 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.

Findings: [ST] Selects a single key encryption mode for FCS_COP.1(g). No additional guidance is required.

5.1.5.3 KMD

159 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.

Findings: [KMD] Figures 2, 3, and 4 indicate that the resulting 256-bit values (SUB1 or KEK1) are used to encrypt the 256-bit BEV using AES-256-GCM.

5.1.5.4 Test

160 The AES test should be followed in FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption.

Findings: The vendor uses the CAVP certificate A4388 for AES-GCM (256 bits) encryption and decryption per ISO/IEC 18033-3 (AES) and ISO/IEC 19772 (GCM). This is described in [ST] Table 4.

5.1.6 FCS_KDF_EXT.1 Cryptographic Key Derivation

5.1.6.1 TSS

161 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.

Findings: [ST] Section 6.2.12 states that passwords are conditioned via PBKDF2 using HMAC-SHA-512 with 111,254 iterations, resulting in a 256-bit key in accordance with NIST

	SP 800-132. For smartcard authentication, the TOE accepts an RNG generated submask in accordance with NIST SP 800-108.

5.1.6.2 Operational Guidance

162 There are no AGD evaluation activities for this SFR.

5.1.6.3 KMD

163 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.

Findings:	[KMD] Table 3 labelled “Key Life-Cycle” notes the “Derivation” in relation to the origin of all keys. Depending on the key type, it is either derived from PBKDF2 (password or smartcard) or PBKDF2 and combined using SHA-256 (password and smartcard).

5.1.6.4 Test

164 There are no test evaluation activities for this SFR.

5.1.7 FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning

5.1.7.1 TSS

165 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.

Findings:	[ST] Section 6.2.14 states that the TOE implements a configurable password policy with the following options: a.) Minimum Length (8 – 128) b) Require at least one uppercase c) Require at least one lowercase d) Require at least one numeric e) Require at least one of the following special characters: (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”) Passwords are conditioned via PBKDF2 using HMAC-SHA-512 with 11,248 iterations, resulting in a 256-bit key in accordance with NIST SP 800-132.

5.1.7.2 Operational Guidance

166 There are no AGD evaluation activities for this SFR.

5.1.7.3 KMD

167 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.

Findings:	[KMD] Section 3.1.1 states that passwords are conditioned via PBKDF2 using HMAC-SHA-512 with 111,254 iterations, resulting in a 256-bit key in accordance with NIST SP 800-132. The evaluator confirmed that all resulting keys match the [ST] claim of 256-bits.

168 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.

Findings:	[KMD] Figure 2 and section 3.1.1 indicate how the password is fed into the PBKDF and confirmed that the settings used match the [ST] selections. The resulting key is a 256-bit key which matches the size of the BEV.

5.1.7.4 Test

169 The evaluator shall also perform the following tests:

170 Test 1: Ensure that the TOE supports passwords/passphrases of a minimum length of 64 characters.

High-Level Test Description
The evaluator added a new user with a 64-character password and observed that the TOE accepted the password. The evaluator then successfully logged in as the user using the 64-character password.
Findings: PASS

171 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.

High-Level Test Description
The evaluator attempted to change the user’s password created in test 1 to a 129-character password and verified that the TOE did not accept the password. The evaluator then attempted to log into the TOE with the 129-character password and confirmed that the login failed. The evaluator the attempted to log into the TOE using the 64-character password set in test 1 and confirmed that the login succeeded since the password did not change. The evaluator then successfully changed the password to a 128-character password and successfully logged into the TOE using the 128-character password.
Findings: PASS

172 Test 3: Ensure that the TOE supports passwords consisting of all characters assigned and supported by the ST author.

High-Level Test Description
The evaluator changed the user's password to a password containing all characters claimed and verified the user successfully logged into the TOE with the new password.
Findings: PASS

5.1.8 FCS_RBG_EXT.1 Random Bit Generation

5.1.8.1 TSS

173 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.

Findings:	[ST] Section 6.2.15 states that the DRNG is expected to provide 256 bits of full entropy from RDRAND/RDSEED to seed OpenSSL which is consistent with the selection in FCS_RBG_EXT.1.2.

5.1.8.2 Operational Guidance

174 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.

Findings:	[AGD] Section 2.2 “Configuration” states that “There are no specific steps required to establish the evaluated configuration.” The TOE uses the DRBG by default.

5.1.8.3 KMD

175 There are no KMD evaluation activities for this SFR.

5.1.8.4 Test

176 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.

177 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).

178 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.

179 The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

180 Entropy input: the length of the entropy input value must equal the seed length.

181 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.

182 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.

183 Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

Findings:	The vendor uses the CAVP certificate A4388 for CTR_DRBG (AES) random bit generation in accordance with NIST SP 800-90A. This is described in [ST] Table 4.

5.1.9 FCS_SMC_EXT.1 Submask Combining

5.1.9.1 TSS

184 If the submasks produced from the authorization factors are XORed together to form the BEV or intermediate key, the TSS section shall identify how this is performed (e.g., if there are ordering requirements, checks performed, etc.). The evaluator shall also confirm that the TSS describes how the length of the output produced is at least the same as that of the BEV.

Findings:	The submasks are not XORed together. [ST] Section 6.2.16 states that the submasks are combined using SHA-256. The resulting 256-bit is equal to the size of the BEV.

5.1.9.2 Operational Guidance

185 There are no AGD evaluation activities for this SFR.

5.1.9.3 KMD

186 The evaluator shall review the KMD to ensure that an approved combination is used and does not result in the weakening or exposure of key material.

Findings:	[KMD] Section 3.1 depicts Figure 4 where submask combining is used. The submask combing uses SHA-256 which results in a 256-bit KEK that does not weaken or expose the 256-bit keys used throughout the keychain.

5.1.9.4 Test

187 The evaluator shall perform the following test:

188 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 encrypted data.

High-Level Test Description
The evaluator performed this test in conjunction with FCS_AFA_EXT.1.
Findings: PASS

6 Evaluation Activities for SARs

6.1 ASE: Security Target Evaluation

6.1.1 ASE_CCL.1 Exact Conformance Actions

6.1.1.1 ASE_CCL.1.8C

189 The evaluator shall check that the statements of security problem definition in the PP and ST are identical.

Findings:	[ST] Section 3 includes the security problem definition from CPP_FDE_AA_V2.0E. The statements of security definition are identical in the PP and the ST.

6.1.1.2 ASE_CCL.1.9C

190 The evaluator shall check that the statements of security objectives in the PP and ST are identical.

Findings:	[ST] Section 4 includes the security objectives from CPP_FDE_AA_V2.0E. The statements of security objectives are identical in the PP and the ST.

6.1.1.3 ASE_CCL.1.10C

191 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.

Findings:	[ST] Section 5 includes the security requirements from the CPP_FDE_AA_V2.0E. All mandatory SFRs in the cPP and all of the selection-based SFRs that are entailed by selections made are present in Section 5 of the [ST]. No optional SFRs are claimed.

6.1.2 Development (ADV)

6.1.2.1 Basic Functional Specification (ADV_FSP.1)

192 The EAs for this assurance component focus on understanding the interfaces (e.g., application programming interfaces, command line interfaces, graphical user interfaces, network interfaces) described in the AGD documentation, and possibly identified in the TOE Summary Specification (TSS) in response to the SFRs. Specific evaluator actions to be performed against this documentation are identified (where relevant) for each SFR in Section 2 (Evaluation Activities for SFRs), and in EAs for AGD, ATE and AVA SARs in other parts of Section 5.

193 The EAs presented in this section address the CEM work units ADV_FSP.1-1, ADV_FSP.1-2, ADV_FSP.1-3, and ADV_FSP.1-5.

194 The EAs are reworded for clarity and interpret the CEM work units such that they will result in more objective and repeatable actions by the evaluator. The EAs in this SD are intended to ensure the evaluators are consistently performing equivalent actions.

195 The documents to be examined for this assurance component in an evaluation are therefore the Security Target, AGD documentation, and any required supplementary information required by the cPP: no additional “functional specification” documentation is necessary to satisfy the EAs. The interfaces that need to be evaluated are also identified by reference to the EAs listed for each SFR, and are expected to be identified in the context of the Security Target, AGD documentation, and any required supplementary information defined in the cPP rather than as a separate list specifically for the purposes of CC evaluation. The direct identification of documentation requirements and their assessment as part of the EAs for each SFR also means that the tracing required in ADV_FSP.1.2D (work units ADV_FSP.1-4, ADV_FSP.1-6 and ADV_FSP.1-7 is treated as implicit and no separate mapping information is required for this element.

6.1.2.1.1 ADV_FSP.1-1

196 The evaluator shall examine the functional specification to determine that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.

197 Evaluation Activity: 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.

Findings:	The evaluator examined the [AGD] and [MAN] (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 verified the [AGD] and [MAN] describes the purpose and method of use for each security relevant TSFI by verifying the [AGD] and [MAN] satisfies all of the Guidance Evaluation Activities.

6.1.2.1.2 ADV_FSP.1-2

198 The evaluator shall examine the functional specification to determine that the method of use for each SFR-supporting and SFR-enforcing TSFI is given.

199 Evaluation Activity: 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.

Findings:	The evaluator examined the [AGD] and [MAN] (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 verified the [AGD] and [MAN] describes the purpose and method of use for each security relevant TSFI by verifying the [AGD] and [MAN] satisfies all of the Guidance Evaluation Activities.

6.1.2.1.3 ADV_FSP.1-3

200 The evaluator shall examine the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR supporting TSFI.

201 Evaluation Activity: 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.

Findings:	The evaluator examined the [AGD] and [MAN] (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 verified the [AGD] and [MAN] describes the purpose and method of use for each security relevant TSFI by verifying the [AGD] and [MAN] satisfies all of the Guidance Evaluation Activities.

6.1.2.1.4 ADV_FSP.1-4

202 The evaluator shall examine the rationale provided by the developer for the implicit categorisation of interfaces as SFR non-interfering to determine that it is accurate.

203 Paragraph 561 from the CEM: "In the case where the developer has provided adequate documentation to perform the analysis called for by the rest of the work units for this component without explicitly identifying SFR-enforcing and SFR supporting interfaces, this work unit should be considered satisfied."

204 Since the rest of the ADV_FSP.1 work units will have been satisfied upon completion of the EAs, it follows that this work unit is satisfied as well.

Findings: As noted above, this work unit is covered with the rest of the ADV_FSP.1 work units.

6.1.2.1.5 ADV_FSP.1-5

205 The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.

206 Evaluation Activity: The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

Findings: The evaluation team examined the interface documentation and was able to map interfaces to SFRs, sufficient to enable each of the evaluation activities to be completed satisfactorily. The evaluation team's results from performing the evaluation activities are documented in Sections 3, 4 and 5 of this document.

6.1.2.1.6 ADV_FSP.1-6

207 The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.

208 EAs that are associated with the SFRs in Section 2, and, if applicable, Sections 3 and 4, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are covered. Therefore, the intent of this work unit is covered.

Findings: As noted above, this work unit is covered with the EAs associated with the SFRs throughout this document.

209 ADV_FSP.1-7

210 The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.

211 EAs that are associated with the SFRs in Section 2, and, if applicable, Sections 3 and 4, are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are addressed, and that the description of the interfaces is accurate with respect to the specification captured in the SFRs. Therefore, the intent of this work unit is covered.

Findings: As noted above, this work unit is covered with the EAs associated with the SFRs throughout this document.

6.1.2.1.7 Evaluation Activity

212 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.

213 In this context, TSFI are deemed security relevant if they are used by the administrator to configure the TOE, or to perform other administrative functions (e.g., audit review or performing updates). Additionally, those interfaces that are identified in the ST, or guidance documentation, as adhering to the security policies (as presented in the SFRs), are also considered security relevant. The intent, is that these interfaces will be adequately tested, and having an understanding of how these interfaces are used in the TOE is necessary to ensure proper test coverage is applied.

214 The set of TSFI that are provided as evaluation evidence are contained in the Administrative Guidance and User Guidance.

Findings:	The assurance activities from Supporting Documents of CPP_FDE_AA_V2.0E have been performed. The evaluator concluded adequate information was provided and the analysis of the evaluator is documented in Sections 3, 4 and 5 of this document.

6.1.2.1.8 Evaluation Activity

215 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.

Findings:	The assurance activities from Supporting Documents of CPP_FDE_AA_V2.0E have been performed. The evaluator concluded adequate information was provided and the analysis of the evaluator is documented in Sections 3, 4, and 5 of this document.

6.1.2.1.9 Evaluation Activity

216 The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

217 The evaluator uses the provided documentation and first identifies, and then examines a representative set of interfaces to perform the EAs presented in Section 2 (Evaluation Activities for SFRs), including the EAs associated with testing of the interfaces.

218 It should be noted that there may be some SFRs that do not have an interface that is explicitly “mapped” to invoke the desired functionality. For example, generating a random bit string, destroying a cryptographic key that is no longer needed, or the TSF failing to a secure state, are capabilities that may be specified in SFRs, but are not invoked by an interface.

219 However, if the evaluator is unable to perform some other required EA because there is insufficient design and interface information, then the evaluator is entitled to conclude that an adequate functional specification has not been provided, and hence that the verdict for the ADV_FSP.1 assurance component is a ‘fail’.

Findings:	The assurance activities from Supporting Documents of CPP_FDE_AA_V2.0E have been performed. The evaluator concluded adequate information was provided and the analysis of the evaluator is documented in Sections 3, 4 and 5 of this document.

6.2 Guidance Documents (AGD)

220 It is not necessary for a TOE to provide separate documentation to meet the individual requirements of AGD_OPE and AGD_PRE. Although the Evaluation Activities in this

section are described under the traditionally separate AGD families, the mapping between real TOE documents and AGD_OPE and AGD_PRE requirements may be many-to-many, as long as all requirements are met in documentation that is delivered to administrators and users (as appropriate) as part of the TOE.

6.2.1 Operational User Guidance (AGD_OPE.1)

221 Specific requirements and checks on the user guidance documentation are identified (where relevant) in the individual Evaluation Activities for each SFR, and for some other SARs (e.g. ALC_CMC.1).

6.2.1.1 Evaluation Activity:

222 The evaluator shall check the requirements below are met by the operational guidance.

223 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.

224 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.

225 The contents of the operational guidance will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in sections 2, 3, and 4 above.

226 In addition to SFR-related Evaluation Activities, the following information is also required.

- 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 TOE will likely contain security functionality that does not fall under 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.

Findings: The evaluator checked the requirements above are met by the guidance documentation. The 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. The CC guidance will also be published on www.niap-ccevs.org.

The evaluator ensured that the Operational guidance is provided for every Operational Environment (OE) that the product supports as claimed in the Security Target. Section 1.3.2 Evaluated Software of the [AGD] specifies the TOE and Section 1.3.3 Non-TOE Components of the [AGD] specifies the supported OE (Non-TOE Components).

The [AGD] Section 2.8 Cryptography states that “The TOE supports a 256-bit DEK using AES-GCM-256. No other configuration of cryptographic parameters is possible/required.”

	The evaluator verified the operational guidance documentation makes it clear which security functionality is covered by the Evaluation Activities.

6.2.2 Preparative Procedures (AGD_PRE.1)

227 As for the operational guidance, specific requirements and checks on the preparative procedures are identified (where relevant) in the individual Evaluation Activities for each SFR.

6.2.2.1 Evaluation Activity:

228 The evaluator shall check the requirements below are met by the preparative procedures.

229 The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in section 2 above.

230 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.

231 The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in section 2 above.

232 In addition to SFR-related Evaluation Activities, the following information is also required.

233 Preparative procedures must include a description of how the 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). The documentation should be in an informal style and should be written with sufficient detail and explanation that they can be understood and used by the target audience (which will typically include IT staff who have general IT experience but not necessarily experience with the TOE itself).

234 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. This may be contained all in one document.

235 The preparative procedures must include

- instructions to successfully install the TSF in each Operational Environment; and
- instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
- instructions to provide a protected administrative capability.

Findings:	The evaluator checked the requirements above are met by the guidance documentation. The 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. The CC guidance will also be published on www.niap-ccevs.org.

The [AGD] following sections describe how the Operational Environment fulfil its role:

- 1.3.2 Evaluated Software

- 1.3.3 Non-TOE Components

- 2 Guidance

Section 1.3.3 Non-TOE Components identifies the supported platforms and OE for the TOE.

The preparative procedures include instructions to get the drive successfully installed are provided in the [AGD] section 2.2 Configuration. This section is accompanied with [MAN] section 2 Initial Installation.

The preparative procedures include instructions to provide a protected administrative capability in the [AGD] section 2.2 Configuration. This section is accompanied with [MAN] section 2 Initial Installation.

6.3 Life-cycle Support (ALC)

6.3.1 Labelling of the TOE (ALC_CMC.1)

236 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.

Findings:	The [ST], TOE and [AGD] are all labelled with the same software version. The information is specific enough to procure the specific TOE software version.

6.3.2 TOE CM coverage (ALC_CMS.1)

237 When evaluating the developer’s coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

Findings:	The [ST], TOE and [AGD] are all labelled with the same software version. The information is specific enough to procure the specific TOE software version.

6.4 Tests (ATE)

6.4.1 Independent Testing – Conformance (ATE_IND.1)

238 Testing is performed to confirm the functionality described in the TSS as well as the operational guidance documentation. The focus of the testing is to confirm that the requirements specified in the SFRs are being met.

239 The evaluator should consult Appendix B FDE Equivalency Considerations when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.

240 The SFR-related Evaluation Activities in the SD identify the specific testing activities necessary to verify compliance with the SFRs. The tests identified in these other Evaluation Activities constitute a sufficient set of tests for the purposes of meeting ATE_IND.1.2E. It is important to note that while the Evaluation Activities identify the testing that is necessary to be performed, the evaluator is responsible for ensuring that the interfaces are adequately tested for the security functionality specified for each SFR.

6.4.1.1 Evaluation Activity:

241 The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

Findings:	The TOE conforms with all configuration elements as specified in the ST.

6.4.1.2 Evaluation Activity:

242 The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.

Findings:	The evaluator verified that the TOE has been installed properly and is in a known state. The evaluator followed the configuration steps found in [AGD]/[MAN] to ensure this was the case.

6.4.1.3 Evaluation Activity:

243 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.

Findings:	The evaluator verified that the test plan covers all of the testing actions found in ATE_IND.1 in the CEM.

244 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.

Findings:	The evaluator verified that the test plan includes and identifies the platforms that need to be tested. The ST claims a single version of the software which was fully tested for all SFRs.

245 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).

Findings:	The evaluator verified that the test plan describes the composition and configuration of each platform to be tested. AGD documentation was followed by the evaluator for installation and setup.

246 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.

Findings: The evaluator verified that the test plan identifies high-level test objectives as well as all test procedures to follow.

247 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.

Findings: The evaluator verified that the test report details activities that took place when all tests were executed

7 Vulnerability Assessment (AVA)

7.1 Vulnerability Survey (AVA_VAN.1)

7.1.1 Vulnerability Survey (AVA_VAN.1) Evaluation Activities

7.1.1.1 AVA_VAN.1-1

248 The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

249 Evaluation Activity: The evaluator shall perform the CEM activity as specified.

250 *If the iTC specifies any tools to be used in performing this analysis in section A.3.4, the following text is also included in this cell: "The calibration of test resources specified in paragraph 1418 of the CEM applies to the tools listed in Appendix A, Section A.1.4."*

7.1.1.2 AVA_VAN.1-2

251 The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.

252 Evaluation Activity: The evaluator shall perform the CEM activity as specified.

7.1.1.3 AVA_VAN.1-3

253 The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.

254 Evaluation Activity: Replace CEM work unit with activities outlined in Appendix A, Section A.1.

7.1.1.4 AVA_VAN.1-4

255 The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.

256 Evaluation Activity: Replace the CEM work unit with the analysis activities on the list of potential vulnerabilities in Appendix A, section A.1, and documentation as specified in Appendix A, Section A.3.

7.1.1.5 AVA_VAN.1-5

257 The evaluator shall devise penetration tests, based on the independent search for potential vulnerabilities.

258 Evaluation Activity: Replace the CEM work unit with the activities specified in Appendix A, section A.2.

7.1.1.6 AVA_VAN.1-6

259 The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include:

a) identification of the potential vulnerability the TOE is being tested for;

b) instructions to connect and setup all required test equipment as required to conduct the penetration test;

c) instructions to establish all penetration test prerequisite initial conditions;

d) instructions to stimulate the TSF;

e) instructions for observing the behaviour of the TSF;

f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;

g) instructions to conclude the test and establish the necessary post-test state for the TOE.

260 Evaluation Activity: The CEM work unit is captured in Appendix A, Section A.3; there are no substantive differences.

7.1.1.7 AVA_VAN.1-7

261 The evaluator shall conduct penetration testing.

262 Evaluation Activity: The evaluator shall perform the CEM activity as specified. See Appendix A, Section A.3 for guidance related to attack potential for confirmed flaws.

7.1.1.8 AVA_VAN.1-8

263 The evaluator shall record the actual results of the penetration tests.

264 Evaluation Activity: The evaluator shall perform the CEM activity as specified.

7.1.1.9 AVA_VAN.1-9

265 The evaluator shall report in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

266 Evaluation Activity: Replace the CEM work unit with the reporting called for in Appendix A, Section A.3.

7.1.1.10 AVA_VAN.1-10

267 The evaluator shall examine the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential.

268 Evaluation Activity: This work unit is not applicable for Type 1 and Type 2 flaws (as defined in Appendix A, Section A.1), as inclusion in this Supporting Document by the iTC makes any confirmed vulnerabilities stemming from these flaws subject to an attacker possessing a Basic attack potential. This work unit is replaced for Type 3 and Type 4 flaws by the activities defined in Appendix A, Section A.3.

7.1.1.11 AVA_VAN.1-11

269 The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each:

a) its source (e.g. CEM activity being undertaken when it was conceived, known to the evaluator, read in a publication);

b) the SFR(s) not met;

c) a description;

d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual).

e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using the tables 3 and 4 of Annex B.4.

270 Evaluation Activity: Replace the CEM work unit with the reporting called for in Appendix A, Section A.3.

271 Because of the level of detail required for the evaluation activities, the bulk of the instructions are contained in Appendix A, while an “outline” of the assurance activity is provided below.

Findings:	As noted above, the evaluation activities for AVA_VAN.1-1 through AVA_VAN.1-11 are performed in conjunction with the activities below.

7.1.1.12 Evaluation Activity (Documentation)

272 The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components apply to all systems claimed in the ST, and should identify at a minimum the processors used by the TOE. Software components include any libraries used by the TOE, such as cryptographic libraries. This additional documentation is merely a list of the name and version number of the components, and will be used by the evaluators in formulating hypotheses during their analysis.

273 The evaluator shall examine the documentation outlined below provided by the vendor to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.

Findings:	The evaluator collected this information from the developer which was used to feed into the Type 1 Flaw Hypotheses search (below).

274 In addition to the activities specified by the CEM in accordance with Table 2 above, the evaluator shall perform the following activities.

7.1.1.13 Evaluation Activity

275 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.

Findings:	The evaluator followed [SD] Appendix A.1, A.2 and A.3 to perform the vulnerability analysis and documented the results in [AVA]. The following sources of public vulnerabilities were considered in formulating the specific list of flaws to be investigated by the evaluators, as well as to reference in

directing the evaluators to perform key-word searches during the evaluation of the TOE. Hypothesis sources for public vulnerabilities were:

NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search

Common Vulnerabilities and Exposures:
https://cve.mitre.org/cve/search_cve_list.html

US-CERT: http://www.kb.cert.org/vuls/html/search

Type 1 Hypothesis searches were last conducted on October 2, 2023 and included the following search terms:

Cigent

Cigent PBA Software v1.0.6.4

Drive encryption

Disk encryption

Key destruction

Key sanitization

Self Encrypting Drive (SED)

OPAL

Key Caching

Opal management software

SED management software

Openssl

Sqlcipher

Zlib

Gzip

Libpcsclite

The evaluation team determined that no residual vulnerabilities exist based on these searches that are exploitable by attackers with Basic Attack Potential.

The [PP] identifies type-2 hypotheses, TOE was not found to be vulnerable. This is documented in [AVA].

No type 3 or type 4 hypotheses were identified by the evaluation team.

NIAP TD0606

276 The NAS should be tested in AVA_VAN.1 to be certain that it is in the claimed evaluated configuration, locally managed with remote management disabled.

Findings: The TOE does not include or make use of a NAS. This is not applicable.