KLC Group LLC

CipherDrive 1.2.2

Assurance Activity Report

Version 1.2

17-Feb-2021

Document prepared by

www.lightshipsec.com

Table of Contents

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security 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	Canadian Common Criteria Scheme
Evaluation Facility	Lightship Security, Inc.
Developer/Sponsor	KLC Group LLC
TOE	CipherDrive v1.2.2 build 7
Security Target	KLC Group LLC CipherDrive v1.2.2 Security Target, v1.1
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201 (referenced within as CPP_FDE_AA)

1.2 Evaluation Methods

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

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1R5
Evaluation Methodology	CEM v3.1R5
Supporting Documents	Supporting Document, Full Drive Encryption: Authorization Acquisition, February 2019, Version 2.0 + Errata 20190201
Interpretations	**CPP_FDE_AA v2.0e** TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities

2 TOE Details

2.1 Overview

1 The TOE is software that provides pre-boot authentication (PBA) for use with a SED.

2.2 Models and Platforms

2 The TOE operates with the following components in the environment:

a) **SED.** Opal 2.0 compliant SED. CC testing performed using SEDs:
   i) Digistor DIG-M25126-SI
   ii) Digistor DIG-M2N22566-UI

b) **Protected OS.** The TOE supports protection of Linux Operating Systems/Linux based Hypervisors and Windows Operating Systems.

c) **Computer Hardware.** Intel based UEFI booted systems. CC Testing performed using CPUs:
   i) Intel Atom x7-E3950
   ii) Intel Core i5-9400H

d) **Smartcard and reader.** When dual factor authentication is used, Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcards and readers are required.

2.3 Reference Documents

Table 3: List of Reference Documents

Ref	Document
[ST]	KLC Group LLC CipherDrive v1.2.2 Security Target, v1.1
[ADMIN]	KLC Group LLC CipherDrive v1.2 KLC PBA, version 1.2.1 (and later), 11-17-2020
[SUPP]	KLC Group LLC CipherDrive v1.2 Common Criteria Guide, v1.1
[KMD]	KLC Group CipherDrive v1.2 Key Management Description, Version 0.4, May 2020

2.4 Summary of SFRs

Table 4: List 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)

Requirement	Title
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)
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

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

3 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.

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

Findings:	The evaluator verified that authorization factors are described in section 6.2.1.1 of the [ST] for password-based factor and section 6.2.1.2 of the [ST] for dual factors (password + smartcard). The evaluator also performed evaluation of FCS_PCC_EXT.1 TSS evaluation activities (refer to verdict for such a SFR).

3.1.1.2 Operational Guidance

5 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:	In the [SUPP] guidance section 2.3, the characteristics of the external authorization factors are described at a high level. For passwords, the reader is referred to the user manual [ADMIN] and for smart cards, the cards must be FIPS201 PIV-CAC compliant.

3.1.1.3 KMD

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

7 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:	The evaluator checked section 3.1 of [KMD] and confirmed that the initial authorization factors (submasks) directly contribute to the unwrapping of the BEV. The evaluator also verified that it describes how a submask is produced from the authorization factor, and length of the submask meets the required size.

3.1.1.4 Test

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

9 The evaluator shall also perform the following tests:

10 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
Configure the TOE to require 2FA. Register a user with a smart card and password. Attempt to login using the wrong PIN on the correct smart card and show it fails. Attempt to login using the wrong key on the correct card and show it fails. Attempt to login using the wrong smart card and show it fails. Permit a user to self-enroll a smart card after first configuring a password. Attempt to login using the wrong PIN on the correct smart card and show it fails. Attempt to login using the wrong key on the correct card and show it fails. Attempt to login using the wrong smart card and show it fails.
PASS

3.1.2 FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition

3.1.2.1 TSS

11 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:	The evaluator examined section 6.2.2 of the [ST] and determined that it states that the user must authenticate via password or dual factor to gain access to user data after the TOE entered a Compliant power saving state. The statement is consistent with FCS_AFA_EXT.1.

3.1.2.2 Operational Guidance

12 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:	Section 2.5 of [SUPP] indicates that the same authorization factors are required to access plaintext data when resuming from a compliant power-saving state.

3.1.2.3 KMD

13 There are no KMD evaluation activities for this SFR.

3.1.2.4 Test

14 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
Boot into the OS using a valid credential. Inside of the OS, execute procedures to enter state S4. Show that when resuming, credentials are required. Provide an invalid smart card PIN and show the OS is not resumed. Provide an invalid smart card key and show the OS is not resumed. Provide an incorrect password but valid key and PIN and show the OS is not resumed. Provide an entirely invalid smart card and show the OS is not resumed. Repeat for G2(S5). For state G3, remove the power cable after the device shuts off. Wait 30 seconds to ensure all capacitors are discharged and plug the cable back in before powering on the device.
PASS

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

3.1.3.1 TSS

15 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:	The evaluator checked section 6.2.4 of the [ST] and determined that it provides high-level description of destruction of keys in volatile memory. Furthermore, sections 3.2 and 3.3 in [KMD] provide proprietary information of key life-cycle and key destruction.

3.1.3.2 Operational Guidance

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

Findings:	The TOE does not rely on the operational environment to clear keys.

3.1.3.3 KMD

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

Findings:	The evaluator checked table 3 in [KMD] and determined that it lists type of key, its origin, possible memory locations in volatile memory.

3.1.3.4 Test

18 There are no test evaluation activities for this SFR.

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

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

19 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.

20 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).

21 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.

22 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:	The evaluator examined [KMD] document (especially, section 3), and determined that it describes how keys are managed in volatile memory and how keys are managed in non-volatile memory.

3.1.4.2 Operational Guidance

23 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.

24 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.

25 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.

26 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.

27 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:	In section 2.4 of [SUPP], there are no situations where key destruction is prevented or delayed.

3.1.4.3 Test

28 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.

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

30 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
Using a debug version of the TOE, perform the actions to unlock the SED. However, before the protected OS is launched, capture an image of RAM for offline analysis. Using the known keys derived from the debug build, search for these keys in the RAM image and show they do not exist. Also, split the keys into three fragments of similar-sized pieces and search for these keys in full in the RAM image and show they do not exist. Repeat for each of the following points of interest: returning from hibernating the protected OS, returning from shutting down the protected OS, and returning from

High-Level Test Description
mechanically shutting down the protected OS. These test cases are due to FPT_PWR_EXT.1 and FPT_PWR_EXT.2.
PASS

31 *The following tests apply only to selection a)[1], since the TOE in this instance has more visibility into what is happening within the underlying platform (e.g., a logical view of the media). In selection b), the TOE has no visibility into the inner workings and completely relies on the underlying platform, so there is no reason to test the TOE beyond test 1.*

32 *For selection a), the following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern.*

33 Test 2: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use a tool that provides a logical view of the media (e.g., MBR file system):

1. Record the value of the key in the TOE subject to clearing.
2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
3. Cause the TOE to clear the key.
4. Search the logical view that the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.
5. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for Use Case 1 test 1 above), and if a fragment is found in the repeated test then the test fails.

NOTE:	The above test is not applicable since the [ST] claims in section 5.3.1 that it destroys the abstraction which represents the key.

34 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.

[1] If the TOE can logically address the storage location of the key rather than just deleting the abstraction that represents the key.

35 The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

NOTE:	The above test is not applicable since the [ST] claims in section 5.3.1 that it destroys the abstraction which represents the key.

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

3.1.5.1 TSS

36 The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

Findings:	The evaluator was directed to [KMD] for required information, and determined that, in section 3.3 of the [KMD], there is high-level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

3.1.5.2 Operational Guidance

37 There are no AGD evaluation activities for this SFR.

3.1.5.3 KMD

38 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.

39 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:	The evaluator checked table 3 in [KMD] and determined that it describes areas where keys and key material reside and when the keys and key material are no longer needed, and it also includes a key lifecycle and key destruction description..

3.1.5.4 Test

40 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

41 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:	The evaluator checked section 6.2.7 in the [ST] and section 3 of the [KMD], and determined that it specifies that all keys and key material in RAM are destroyed when entering any Compliant power saving state.

3.1.6.2 Operational Guidance

42 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:	In section 2.1 of [SUPP], there are clear instructions to disable non-compliant power states. The supported power states are further described in section 2.5 of [SUPP] and these use consistent technical terms that IT and security administrators can use to unambiguously identify power states within a host OS.

3.1.6.3 KMD

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

44 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:	The evaluator checked section 3.2 and table 3 in [KMD], and determined that it describes areas where keys and key material reside and when the keys and key material are no longer needed, and it also includes a key lifecycle and key destruction description.

3.1.6.4 Test

45 There are no test evaluation activities for this SFR.

3.1.7 FCS_KYC_EXT.1 Key Chaining (Initiator)

3.1.7.1 TSS

46 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:	The evaluator checked sections 6.1.2 and 6.2.13 of the [ST] and determined that there is a high-level description of BEV sizes.

3.1.7.2 Operational Guidance

47 There are no AGD evaluation activities for this SFR.

3.1.7.3 KMD

48 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.

49 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.

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

Findings:	The evaluator checked section 3.1 in [KMD] and determined that it provides a high level description of the key hierarchy for all authorizations methods selected in FCS_AFA_EXT.1 that are used to protect the BEV..

3.1.7.4 Test

51 There are no test evaluation activities for this SFR.

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

3.1.8.1 TSS

52 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.

53 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:	The evaluator checked section 6.2.17 of the [ST] and determined that it describes how salts and IVs are generated. Note that TOE does not make use of nonces.

3.1.8.2 Operational Guidance

54 There are no AGD evaluation activities for this SFR.

3.1.8.3 KMD

55 There are no KMD evaluation activities for this SFR.

3.1.8.4 Test

56 There are no test evaluation activities for this SFR.

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

3.1.9.1 TSS

57 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:	The evaluator checked sections 6.2.3 and 6.1.2 of the [ST] and determined that they describe what symmetric keys are supported, how keys are protected, as well as supported key sizes.

3.1.9.2 Operational Guidance

58 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:	The selection of appropriate key sizes is not configurable.

3.1.9.3 KMD

59 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:	The evaluator checked section 3.1 in [KMD] and determined that it details how the symmetric key is used as part of the key chain.

3.1.9.4 Test

60 There are no test evaluation activities for this SFR.

Findings:	Claimed symmetric cryptographic algorithms (AES-CBC 128- and 256-bits) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

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

3.1.10.1 TSS

61 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:	The evaluator checked section 6.2.8 of the [ST] and determined that it describes the overall flow of the signature verification.

3.1.10.2 Operational Guidance

62 There are no AGD evaluation activities for this SFR.

3.1.10.3 KMD

63 There are no KMD evaluation activities for this SFR.

3.1.10.4 Test

Findings:	Claimed signature verification algorithms (RSA 4096-bit) are provided by CAVP certificate A972 (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=33573).

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

3.1.11.1 TSS

64 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:	The evaluator checked section 6.2.9 of the [ST] and determined that the association of the hash function with other TSF cryptographic functions is described.

3.1.11.2 Operational Guidance

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

Findings:	The selection of appropriate hash sizes is not configurable.

3.1.11.3 KMD

66 There are no KMD evaluation activities for this SFR.

3.1.11.4 Test

Findings:	Claimed cryptographic hashing algorithms (SHA2-512) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

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

3.1.12.1 TSS

67 If HMAC was selected:

68 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.

69 If CMAC was selected:

70 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:	The evaluator checked section 6.2.10 of the [ST] and determined that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

3.1.12.2 Operational Guidance

71 There are no AGD evaluation activities for this SFR.

3.1.12.3 KMD

72 There are no KMD evaluation activities for this SFR.

3.1.12.4 Test

Findings:	Claimed cryptographic keyed-hashing algorithms (HMAC-SHA2-512) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

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

3.1.13.1 TSS

73 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:	The evaluator checked section 6.2.11 of the [ST] and verified that it includes a description of the key size used for encryption and the mode used for the key encryption.

3.1.13.2 Operational Guidance

74 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:	The selection of encryption modes is not configurable.

3.1.13.3 KMD

75 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:	The evaluator checked section 3.1 in [KMD] and determined that it details how key encryption is used as part of the key chain.

3.1.13.4 Test

Findings:	Claimed key encryption algorithms (encryption of keys using AES-CBC-256) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

3.1.14 FCS_KDF_EXT.1 Cryptographic Key Derivation

3.1.14.1 TSS

76 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:	The evaluator checked section 6.2.12 of the [ST] and verified that it includes a description of the key derivation function and the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-132.

3.1.14.2 Operational Guidance

77 There are no AGD evaluation activities for this SFR.

3.1.14.3 KMD

78 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:	The evaluator checked section 3.1 and table 3 in [KMD], and determined that it describes how approved methods are used for key derivation and how / when keys are derived.

3.1.14.4 Test

Findings:	Claimed key derivation algorithms (PBKDF2 using HMAC-SHA-512) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

79 There are no test evaluation activities for this SFR.

3.1.15 FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning

3.1.15.1 TSS

80 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:	The evaluator checked section 6.2.14 of the [ST] and verified that it describes the options of password construction, including the length, and requirements on characters (number and type); it also describes how the password is conditioned.

3.1.15.2 Operational Guidance

81 There are no AGD evaluation activities for this SFR.

3.1.15.3 KMD

82 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.

83 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:	The evaluator checked section 3.1 in [KMD], and also reviewed section 6.2.12 of the [ST] and determined that the formation of the BEV and intermediary keys is described and that the key sizes match that selected by the ST author. Passwords are conditioned via PBKDF2 using HMAC-SHA-512 with 100,000 iterations, resulting in a 256-bit key in accordance with NIST SP 800-132.

3.1.15.4 Test

84 The evaluator shall also perform the following tests:

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

High-Level Test Description
Boot into the PBA. Navigate to the ‘Users’ section and change the password for a user to be 64 characters long. Then attempt to log into the OS as that user with the old password and show it fails. Use the new password and show it works.
PASS

86 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
Boot into the PBA. Navigate to the ‘Users’ section and change the password for a user to be 129 characters long and show the change attempt fails.
PASS

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

High-Level Test Description
Boot into the PBA. Navigate to the 'Users' section and change the password for a user to use all claimed characters. Then attempt to log into the OS as that user with the new password to show it works.
PASS

3.1.16 FCS_RBG_EXT.1 Random Bit Generation

3.1.16.1 TSS

88 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:	The evaluator checked section 6.2.15 of the [ST] and verified that the TOE does not use RBG services provided by a third party.

3.1.16.2 Operational Guidance

89 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:	The selection of appropriate DRBGs is not configurable.

3.1.16.3 KMD

90 There are no KMD evaluation activities for this SFR.

3.1.16.4 Test

Findings:	Claimed DRBG algorithms (CTR_DRBG) are provided by CAVP C1980: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=12790.

3.1.17 FCS_SMC_EXT.1 Submask Combining

3.1.17.1 TSS

91 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 evaluator checked sections 6.2.16 and 6.1.2 of the [ST], and verified that they describe how submasks produced from the authorization factors are XORed

	together to form the BEV or intermediate key and how the length of the output produced is at least the same as that of the BEV.

3.1.17.2 Operational Guidance

92 There are no AGD evaluation activities for this SFR.

3.1.17.3 KMD

93 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:	The evaluator checked section 3.1 in [KMD] and determined that an approved combination is used and it does not result in the weakening or exposure of key material.

3.1.17.4 Test

94 The evaluator shall perform the following test:

95 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.

NOTE:	This test was performed as part of FCS_AFA_EXT.1 and FCS_AFA_EXT.2 testing.

3.2 Security Management (FMT)

3.2.1 FMT_MOF.1 Management of Functions Behavior

3.2.1.1 TSS

96 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:	The evaluator checked section 6.3.1 of the [ST] and determined that, because the TOE does not allow any modification related to power saving states, this work unit is satisfied.

3.2.1.2 Operational Guidance

97 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 any modification related to power saving states.

3.2.1.3 KMD

98 There are no KMD evaluation activities for this SFR.

3.2.1.4 Test

99 The evaluator shall perform the following tests:

100 Test 1: The evaluator presents a privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior and properties are allowed.

NOTE:	The TOE does not allow any modification related to power saving states.

101 Test 2: The evaluator presents a non-privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior are not allowed.

NOTE:	The TOE does not allow any modification related to power saving states.

3.2.2 FMT_SMF.1 Specification of Management Functions

3.2.2.1 TSS

102 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.

103 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.

104 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.

105 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.

106 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:	The evaluator verified that section 6.3.2 of the [ST] contains a high-level description of management functions and it is consistent with selection in FMT_SMF.1.1.

3.2.2.2 Operational Guidance

107 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:	Section 2.6 of the [SUPP] points the administrator to the appropriate sections within the [ADMIN] documentation. These sections describe how to change the DEK or erase the DEK via the appropriate section in the “Settings Console” under the “Maintenance” screen.

108 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:	Section 2.6 of the [SUPP] points the administrator to the appropriate section within the [ADMIN] documentation. User authorization factors can be changed within the "Users" section of the "Settings Console". Users can self-service or appropriate administrative users can alter these factors.

109 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:	Section 2.6 of the [SUPP] points the administrator to the appropriate section within the [ADMIN] documentation. The TOE can be upgraded using the "Update PBA" option under the "Maintenance" screen.

110 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:	The TOE does not have default authorization factors.

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

Findings:	Section 2.10 in [SUPP] offers guidance on disabling key recovery. This functionality can be disabled at install time, or the functionality can be administratively disabled through the configuration settings after install, and during run-time. Both configurations were tested.

112 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:	The TOE does not allow any modification related to power saving states.

3.2.2.3 KMD

113 There are no KMD evaluation activities for this SFR.

3.2.2.4 Test

114 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
Write a known 32-byte random value to the protected OS. Use the PBA "Change DEK" function to change the DEK. The protected data is erased, but a new DEK is used. Unlock the drive and search for any instances of the 32-byte random value. It will not exist.

High-Level Test Description
Repeat this test for erasing the DEK as well.
PASS

115 If item c) is selected in FMT_SMF.1.1: The evaluator shall initialize the TOE such that it requires the user to input an authorization factor in order to access encrypted data.

Test 1: The evaluator shall first provision user authorization factors, and then verify all authorization values supported allow the user access to the encrypted data. Then the evaluator shall exercise the management functions to change a user's authorization factor values to a new one. Then he or she will verify that the TOE denies access to the user's encrypted data when he or she uses the old or original authorization factor values to gain access.

High-Level Test Description
Our (augmented) test cases in FCS_AFA_EXT.1 and FCS_AFA_EXT.2 show successful access when correct credentials (password and smart card) are provided. Our (augmented) FCS_PCC_EXT.1 test case shows a failed access attempt to reuse an old password after changing the password credential. Building upon those two test cases, we will complete the testing by changing a smart card credential and showing that use of the old password or smart card credential fails.
PASS

116 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.

NOTE:	Please refer to FPT_TUD_EXT.1.

117 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
In previous tests, we have already shown enforcement of smart cards and passwords. For this test case, we will disable the need for a second factor and use a password only and show it is successful.
PASS

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

NOTE:	There are no default authorization factors.

119 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
Log into the device as the Administrator. Show that there are TSF-visible administrative controls to permit key recovery and export set by default or not depending on the means of initial installation. Log into the device as the Security Officer. Show that there are TSF-visible administrative controls to permit key recovery and export. Disable key recovery and then log back in as the Administrator and show that there are no TSF-visible administrative controls to permit key recovery and export.
PASS

120 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.

NOTE:	The TOE does not provide this functionality.

121 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.

NOTE:	The TOE does not provide this functionality.

3.2.3 FMT_SMR.1 Security Roles

3.2.3.1 TSS

122 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

123 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

124 There are no KMD evaluation activities for this SFR.

3.2.3.4 Test

125 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

3.3.1.1 TSS

126 *TD0458*

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

Findings:	The evaluator checked sections 6.1.2 and 6.4.1 in the [ST] and verified that they describe methods used to protect keys in non-volatile memory.

3.3.1.2 Operational Guidance

128 There are no AGD evaluation activities for this SFR.

3.3.1.3 KMD

129 *TD0458*

130 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:	The evaluator checked section 3.1 and table 3 in the [KMD], and determined that they describe the storage location of all keys and the protection of all keys stored in non-volatile memory.

3.3.1.4 Test

131 There are no test evaluation activities for this SFR.

3.3.2 FPT_PWR_EXT.1 Power Saving States

3.3.2.1 TSS

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

Findings:	The evaluator verified that a list of supported compliant power saving states is provided in section 6.4.2 of the [ST].

3.3.2.2 Operational Guidance

133 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:	The set of compliant power-saving states is described in section 2.5 of [SUPP]. The [SUPP] provides instructions to the administrator to disable 'Sleep' mode in the Host OS. The TOE itself does not offer any ability to configure power-saving states.

3.3.2.3 KMD

134 There are no KMD evaluation activities for this SFR.

3.3.2.4 Test

135 The evaluator shall confirm that for each listed compliant state all key/key materials are removed from volatile memory by using the test defined in FCS_CKM.4(d).

NOTE:	This was conducted as part of FCS_CKM.4(d) testing.

3.3.3 FPT_PWR_EXT.2 Timing of Power Saving States

3.3.3.1 TSS

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

Findings:	The evaluator verified that a list of conditions under which TOE enters a compliant power saving state is provided in section 6.4.3 of the [ST].

3.3.3.2 Operational Guidance

137 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:	The set of compliant power-saving states is described in section 2.5 of [SUPP]. The TOE itself does not offer any ability to configure power-saving states. Rather, as per section 2.5 of [SUPP], "[u]sers interact with the Host OS or hardware platform to enter the above power states. Refer to the Host OS guidance for instructions on entering the above power states." Power-loss is explicitly denoted in section 2.5 of [SUPP] as being equivalent to power state G3, which is a supported compliant power-saving state.

3.3.3.3 KMD

138 There are no KMD evaluation activities for this SFR.

3.3.3.4 Test

139 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).

NOTE:	This was conducted as part of FCS_CKM.4(d) testing.

3.3.4 FPT_TUD_EXT.1 Trusted Update

3.3.4.1 TSS

140 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.

141 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:	The evaluator checked section 6.4.4 of the [ST] and determined that it describes information stating that an authorized source signs TOE updates and will have an associated digital signature. Meanwhile, section 6.2.8 of the [ST] also provides relevant information of digital signature based trusted update.

3.3.4.2 Operational Guidance

142 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:	According to [SUPP] section 2.7, updates to the TOE are acquired via the vendor website. Software updates are digitally signed and the TOE automatically verifies the signature prior to installing an update. If signature verification fails, then the update is aborted and an error message is displayed “PBA Upgrade has failed”. In [ADMIN] section “Product upgrade to a new version”, the TOE will power off after a successful upgrade.

3.3.4.3 KMD

143 There are no KMD evaluation activities for this SFR.

3.3.4.4 Test

144 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):

145 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
Perform the following upgrades and expect each to fail: - Modified image with good signature - Signed with an incorrect private key

High-Level Test Description
- Signed with a key of unsupported size - Signed with mangled signature file - Unsigned
PASS

146 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
Use a known-good image and known-good signature and upgrade the TOE. Show that the version number has changed.
PASS