Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

1 Introduction

These errata apply to the "Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015" (hereinafter referred to as the "HCD-PP 1.0") and intend to correct editorial errors mainly in relation to the SFR definition. The "Summary of Changes" and "Detailed Errata" are described in the next chapter and the subsequent chapters.

While using these errata after applying the contents to the HCD-PP 1.0, the ST author shall refer to these errata in the conformance claims of STs (conformance to PPs), along with the HCD-PP 1.0.

(An example of description when claiming conformance in the Security Target)

PP Claim

This ST and TOE claim conformance to the following PP;

PP Name:	*Protection Profile for Hardcopy Devices*
PP Version:	*1.0 dated September 10, 2015*
Errata:	*Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017*

2 Summary of Changes

The contents of the changes in these errata are summarized below.

3.1 Notation error corrections:

Error corrections on the application of "4.1 Notational Conventions (P.34)" in the HCD-PP 1.0 in relation to the SFR definition.

3.2 Extended Component Definition:

Additions of rationales to the Extended SFR Definition (reasons for the need of extended SFRs) in the HCD-PP 1.0.

3.3 Missing Definition of Terms:

Additions of some definitions of terms to the "Appendix G Terminology (P.196)" in the HCD-PP 1.0.

3.4 Dependencies of SFRs:

Error corrections in relation to the definition of the dependencies in the SFR definitions in the HCD-PP 1.0.

3 Detailed Errata

Editorial errors, including Notation convention errors, Extended Component Definition errors, Dependencies inconsistency and missing definitions of terminologies are found in the course of evaluation of the Protection Profile for hardcopy Devices v1.0, and the following changes are to be made to the SFRs in the HCD PP v1.0. Actual changed text is marked with a change bar;

3.1 Notation error corrections

The following texts are the description on Notational Conventions in the HCD PP v1.0 for reference:

Notational Conventions

Bold typeface indicates the portion of an SFR that has been completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or to its Extended Component Definition.

Italic typeface indicates the text within an SFR that must be selected and/or completed by the ST Author in a conforming Security Target.

Bold italic typeface indicates the portion of an SFR that has been partially completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or to its Extended Component Definition. These also must be selected and/or completed by the ST Author in a conforming Security Target.

SFR components that are followed by a letter in parentheses, e.g., (a), (b)… represent required iterations.

Extended components are identified by "_EXT" appended to the SFR identifier.

3.1.1 Class FCS: Cryptographic Support

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or~~
~~FDP_ITC.2 Import of user data with security attributes, or~~
~~FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [selection:

- ***Digital Signature Algorithm (DSA) with key sizes (modulus) of [assignment: 2048 bits or greater],***
- ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [assignment: 2048 bits or greater], or***

- ***Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of [assignment: 256 bits or greater]]***

that meets the following **[selection:**

~~Case: Digital Signature Algorithm~~

~~• FIPS PUB 186-4, "Digital Signature Standard"~~

~~Case: RSA Digital Signature Algorithm~~

~~• FIPS PUB 186-4, "Digital Signature Standard"~~

~~Case: Elliptic Curve Digital Signature Algorithm~~

~~· FIPS PUB 186-4, "Digital Signature Standard"~~

~~• The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").~~

Case: Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***

Case: RSA Digital Signature Algorithm

- ***FIPS PUB 186-4, "Digital Signature Standard"***

Case: Elliptic Curve Digital Signature Algorithm

· FIPS PUB 186-4, "Digital Signature Standard"

- ***The TSF shall implement "NIST curves" P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard").***

].

FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) (selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) Refinement: The TSF shall perform ~~keyed-hash message authentication~~ **keyed-hash message authentication** in accordance with a specified cryptographic algorithm ~~HMAC~~ **HMAC**-[selection: ~~*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*~~***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], **key size** [assignment: ~~*key size (in bits) used in HMAC*~~ **key size (in bits) used in HMAC**], ~~and message digest sizes [selection: *160, 224, 256, 384, 512*] bits~~ **and message digest sizes [selection: *160, 224, 256, 384, 512*] bits** that meet the following: ~~FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."~~**FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication) (selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_COP.1(c) Cryptographic operation (Hash Algorithm), FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(h) Refinement: The TSF shall perform [**keyed-hash message authentication**] in accordance with [**selection:** ~~*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*~~***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512***] and cryptographic key sizes [assignment: ~~*key size (in bits) used in HMAC*~~ ***key size (in bits) used in HMAC***] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2" ; ISO/IEC 10118**].

There is no difference between SFR and its ECD in FCS_CKM_EXT.4, therefore text in Bold typeface should be in default NORMAL typeface as following:

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy ~~**all plaintext secret and private cryptographic keys and cryptographic critical security parameters**~~ all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

The text "destroy" and "destruction" in FCS_CKM.4 are same text as SFR in CC Part2, so these two words should be changed to be in default NORMAL typeface as following:

FCS_CKM.4 Cryptographic key destruction
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM.4.1 Refinement: The TSF shall ~~**destroy**~~ destroy cryptographic keys in accordance with a specified cryptographic key ~~**destruction**~~ destruction method [~~selection~~ **selection**:

~~**For volatile memory, the destruction shall be executed by [selection: *powering off a device*, [assignment: *other mechanism that ensures keys are destroyed*]].**~~

~~**For nonvolatile storage, the destruction shall be executed by a [selection: *single, three or more times*] overwrite of key data storage location consisting of [selection: *a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern*], followed by a [selection: *read-verify*, *none*]. If read-verification of the overwritten data fails, the process shall be repeated again;**~~

For volatile memory, the destruction shall be executed by [selection: powering off a device, [assignment: other mechanism that ensures keys are destroyed]].

For nonvolatile storage, the destruction shall be executed by a [selection: single, three or more times] overwrite of key data storage location consisting of [selection: a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), a static pattern], followed by a [selection: read-verify, none]. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: [**selection:** ***NIST SP800-88, no standard***].

There is no difference between SFR and its ECD in FCS_SNI_EXT.1, therefore text in Bold typeface should be in default NORMAL typeface as following:

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

(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)

Hierarchical to: No other components

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a ~~**RNG as specified in FCS_RBG_EXT.1**~~ RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [

- CBC: IVs shall be non-repeating,
- CCM: Nonce shall be non-repeating.
- XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,
- GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.

].

3.1.2 Class FAU: Security Audit

FAU_GEN.1 Audit data generation
(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the **not specified** level of audit; and
c) ~~All auditable events specified in Table 1,~~ **All auditable events specified in Table 1,** [assignment: other specifically defined auditable events].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 1,** [assignment: other audit relevant information].

Table 1 Auditable Events

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

3.1.3 Class FMT: Security Management

The portions of an SFR that has been completed in this protection profile are required to be in **Bold** typeface. The Authorized roles and Data in Table 4 should be in **Bold** typeface as following:

FMT_MTD.1 Management of TSF data
(for O.ACCESS_CONTROL)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 4.**

Table 4 Management of TSF Data

Data	Operation	Authorised role(s)
[assignment: *list of TSF Data* ~~*owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL*~~ ***owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	~~U.ADMIN, the owning U.NORMAL.~~ **U.ADMIN, the owning U.NORMAL.**
[assignment: *list of TSF Data* ~~*not owned by a U.NORMAL*~~ ***not owned by a U.NORMAL***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	~~U.ADMIN~~ **U.ADMIN**
[assignment: ***list of software, firmware, and related configuration data***]	[selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]	~~U.ADMIN~~ **U.ADMIN**

SFR FMT_SMF.1 is same as SFR in CC Part 2, therefore there is no refinement in FMT_SMF.1. So text "Refinement:" in FMT_SMF.1 should be removed in order to avoid any confusions as following:

FMT_SMF.1 Specification of Management Functions
(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 ~~**Refinement:**~~ The TSF shall be capable of performing the following management functions: [assignment: *list of management functions provided by the TSF*].

3.1.4 Class FPT: Protection of the TSF

Refined extended SFR should specify the portion of text in Bold typeface as following:

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
(for O.KEY_MATERIAL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 Refinement: The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

3.1.5 Class FTP: Trusted Path/Channels

Refined part of SFR should be in Bold typeface as following:

FTP_ITC.1 Inter-TSF trusted channel
(for O.COMMS_PROTECTION, O.AUDIT)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1 Refinement: The TSF shall **use [selection: *IPsec, SSH, TLS, TLS/HTTPS*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**
FTP_ITC.1.2 **Refinement:** The TSF shall permit **the TSF, or the authorized IT entities,** to initiate communication via the trusted channel
FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [assignment: ***list of services for which the TSF is able to initiate communications***].

FTP_TRP.1(a) Trusted path (for Administrators)
(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) Refinement: The TSF shall **use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data.**
FTP_TRP.1.2(a) Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path
FTP_TRP.1.3(a) Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions.**

FTP_TRP.1(b) Trusted path (for Non-administrators)
(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) Refinement : The TSF shall **use [selection,** ***choose at least one of: IPsec, SSH, TLS, TLS/HTTPS*****] to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data.**
FTP_TRP.1.2(b) Refinement: The TSF shall permit [selection: ***the TSF, remote users***] to initiate communication via the trusted path
FTP_TRP.1.3(b) Refinement: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

3.2 Extended Component Definition

The rationale for FCS_KDF_EXT in ECD section is missing. Rationale should be included as following:

FCS_KDF_EXT Extended: Cryptographic Key Derivation

Family Behavior

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

Component leveling

FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Hierarchical to:	No other components
Dependencies:	FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication), [if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108* [selection: *KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

Rationale:

The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.

This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

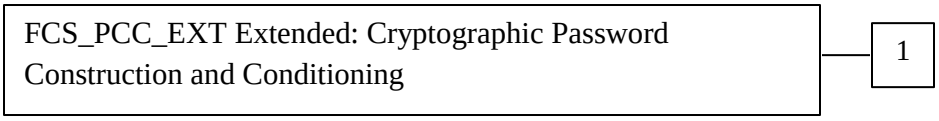
The rationale for FCS_PCC_EXT in ECD section is missing. Rationale should be included as following:

FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning

Family Behavior

This family ensures that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

Component leveling



FCS_PCC_EXT.1 Cryptographic Password Construction and Conditioning, requires the TSF to accept passwords of a certain composition and condition them appropriately.

Management:

No specific management functions are identified

Audit:

There are no auditable events foreseen.

FCS_PCC_EXT.1 Extended: Cryptographic Password Construction and Conditioning

Hierarchical to:	No other components
Dependencies:	FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

FCS_PCC_EXT.1.1 A password used to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [*HMAC*-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] that meet the following: [assignment: *PBKDF recommendation or specification*].

Rationale:

The TSF is required to ensure that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

This extended component protects the Data Encryption Keys using cryptographic algorithms and Robust BEV in the maintained key chains, and it is therefore placed in the FCS class with a single component.

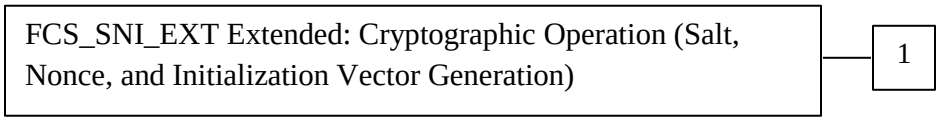
The rationale for FCS_SNI_EXT in ECD section is missing, and there is a notation error. Rationale should be included and a part of text in SFR should be in normal typeface as following:

FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

Family Behavior

This family ensures that salts, nonces, and IVs are well formed.

Component leveling



FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation), requires the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

Management:

No specific management functions are identified

Audit:

There are no auditable events foreseen.

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

Hierarchical to:	No other components
Dependencies:	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a ~~**RNG as specified in FCS_RBG_EXT.1**~~ RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [

CBC: IVs shall be non-repeating,

CCM: Nonce shall be non-repeating.

XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,

GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.

].

Rationale:

The TSF is required to ensure that the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

This extended component protects the communication data and storage data using cryptographic algorithms with specified Salt, Nonce and Initialization Vector Generation, and it is therefore placed in the FCS class with a single component.

Inconsistency between ECD and Selection-base SFR for FCS_IPSEC_EXT.1.5 should be resolved, therefore element FCS_IPSEC_EXT.15 in ECD section should be corrected as following:

FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior

This family addresses requirements for protecting communications using IPsec.

Component leveling

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:

The following actions could be considered for the management functions in FMT:

· There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

· Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message

authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109,* [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], *and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996 ~~(with mandatory support for NAT traversal as specified in section 2.23), 4307~~ [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23], and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on [selection: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)), [assignment: other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.

3.3 Missing Definition of Terms

Following definition of terms and sources need to be appended within the Table 18, Glossary:

Term	Definition	Source
BEV (Border Encryption Value)	A secret value passed to a storage encryption component such as a self-encrypting storage device.	[CPP_FDE_EE_V2.0]
intermediate key	A key used in a point between the initial user authorization and the DEK.	[CPP_FDE_EE_V2.0]
submask	A submask is a bit string that can be generated and stored in a numbers of ways, such as passphrases, tokens, etc.	[CPP_FDE_EE_V2.0]

Sources:

[CPP_FDE_EE_V2.0] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0, September 09, 2016

3.4 Dependencies of SFRs

Inconsistent dependencies in SFR should be corrected as following:

FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification) ~~]~~
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Inconsistent dependencies are found in some of Extended Component Definitions and should be corrected as followings:

FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption) ~~]~~
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Rationale: FCS_CKM.1(b) includes FCS_COP.1(f) only in HCD PP v1.0 but there are three SFRs other than FCS_COP.1(f) such as FCS_COP.1(a), (d) and (e). For consistency, they are appended in its dependencies list.

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation~~
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Rationale: There are two SFRs for FCS_CKM.1 such as for symmetric keys and asymmetric keys. ST authors need to identify the appropriate SFR, i.e. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), for dependencies in ECD section of FCS_COP.1(b) for signature generation/verification.

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit

Generation)

Rationale: According to the cPP for Network devices v1.0, there is FCS_IPSEC_EXT.1 related SFR with some dependencies. For consistency between other cPPs/PPs and HCD PP v1.0, missing SFRs are appended in its dependencies list.

FCS_HTTPS_EXT.1 Extended: HTTPS selected
(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: ~~No dependencies.~~ FCS_TLS_EXT.1 Extended: TLS selected

Rationale: According to the cPP for Network devices v1.0, there is FCS_HTTPS_EXT.1 related SFR with some dependencies. For consistency between other cPPs/PPs and HCD PP v1.0, missing SFRs are appended in its dependencies list.

FCS_SSH_EXT.1 Extended: SSH selected
(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: ~~No dependencies.~~ FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Rationale: According to the cPP for Network devices v1.0, there is FCS_SSH_EXT.1 related SFR with some dependencies. For consistency between other cPPs/PPs and HCD PP v1.0, missing SFRs are appended in its dependencies list.

FCS_TLS_EXT.1 Extended: TLS selected
(selected in FTP_ITC.1.1, FTP_TRP.1.1)

Hierarchical to: No other components.

Dependencies: ~~No dependencies.~~ FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Rationale: According to the cPP for Network devices v1.0, there is FCS_TLS_EXT.1 related SFR with some dependencies. For consistency between other cPPs/PPs and HCD PP v1.0, missing SFRs are appended in its dependencies list.

FPT_TUD_EXT.1 Trusted Update
(for O.UPDATE_VERIFICATION)

Hierarchical to: No other components.

Dependencies: ~~[~~FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), ~~or~~
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)~~]~~.

Rationale: Dependency FCS_COP.1(c) is mandatory for signature verification.