COMBITECH	***TEST REPORT*** *issued by an Accredited Testing Laboratory*	SWEDAC ACKREDITERING Ackred. nr. 1914 Provning ISO/IEC 17025	Ref. No/Order No 1 (106) CAB-240328-124052-475
Unit/Issued by IIQTEA/ Anders Staaf	Date 2024-03-28		Distribution NIAP
Unit/Appoint IIQTEA/ Magnus Ahlbin	Classification UNCLASSIFIED		

Subject

Assurance Activity Report – Kyocera TASKalfa MZ4000i with Hard Disk, FAX System and Data Security Kit

Version number	File name	Product name	Sponsor
1.0	AAR Kyocera TASKalfa MZ4000i HCD-PP v10.pdf	TASKalfa MZ4000i, TASKalfa MZ3200i, TASKalfa M30040i, TASKalfa M30032i(KYOCERA), CS MZ4000i, CS MZ3200i(Copystar), 4063i, 3263i (TA Triumph-Adler/UTAX), with Hard Disk, FAX System and Data Security Kit	Kyocera Document Solution Inc.

Prepared by

Combitech AB
Gustavslundsvägen 42,
SE-167 51 Bromma,
Sweden

Contents

Document history

Date	Ver.	Status	Description	Author
2024-03-28	1.0	Approved	First version	Anders Staaf

The Developer of the TOE

Kyocera Document Solution Inc., 2-28, 1-Chome, Tamatsukuri, Chuo-ku Osaka, Japan.

Common Criteria versions

Common Criteria, version 3.1, revision 5 [CCpart1], [CCpart2], [CCpart3].

Common Evaluation Methodology Versions

Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5 [CEM].

Protection Profiles

Protection Profile for Hardcopy Devices, version 1.0, September 10, 2015, Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017.

NIAP Technical Decisions

In addition to the Protection Profile identified above, the following technical decisions have been applied:

NIAP Technical Decisions	Implementation
0642 - FCS_CKM.1(a) Requirement; P-384 keysize moved to selection	See FCS_CKM.1.1(a) and FCS_COP.1.1(b) in section 2.2
0562 - Test activity for Public Key Algorithms	N/A. The SFR concerned is not included in ST.
0494 - Removal of Mandatory SSH Ciphersuite for HCD	N/A. The SFR concerned is not included in ST.
0474 - Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1	N/A. The SFR concerned is not included in ST.
0393 - Require FTP_TRP.1(b) only for printing	N/A. The TOE is neither a copy-only or a scan-only device.
0299 - Update to FCS_CKM.4 Assurance Activities	N/A. No keys are stored in non-volatile memory according to ST.
0261 - Destruction of CSPs in flash	See FCS_CKM.4 in section 2.2.
0253 - Assurance Activities for Key Transport	N/A. The SFR concerned is not included in ST.
0219 - NIAP Endorsement of Errata for HCD PP v1.0	The errata is refered to by the ST author.
0176 - FDP_DSK_EXT.1.2 - SED Testing	N/A. TOE does not use SED.
0157 - FCS_IPSEC_EXT.1.1 - Testing SPDs	See FCS_IPSEC_EXT.1.1 in section 2.2

Table 1, NIAP Technical Decisions

1 Introduction

This document presents assurance activity evaluation results of the TOE evaluation.

There are four types of assurance activities and the following is provided for each:

- TOE Summary Specification (TSS) - An indication that the required information is in the TSS section of the Security Target;
- Guidance - A specific reference to the location in the guidance is provided for the required information;
- Test – A summary of the test procedure used and the results obtained is provided for each required test activity; and
- KMD - Key Management Description.

This Assurance Activities Report contains sections for each functional class and family and sub-sections addressing each of the SFRs specified in the Security Target [ST].

1.1 References

[PP]	Protection Profile for Hardcopy Device, IPA, NIAP, and the MFP Technical Community, Version 1.0, September 10, 2015
[ST]	TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk, FAX System Security and Target Data Security Kit, version 1.0, October 13, 2023
[ADV_1]	WC4S Software Development WC4S Security Function Specifications for HCD-PP, version 1.00, January 23, 2023, Internal Use Only
[ADV_2]	WiseCore4S Software Development Security Function Specifications TSFI List for HCD-PP, version 0.90, May 13, 2021, Confidential
[CCRX]	Command Center RX User Guide, CCRXKDEN28, May 2022
[CIL]	WC4S_Software Development 2ZS HCD-PP CC Certification TOE Configuration List, version 0.93, December 6, 2022, Confidential
[DevSetup]	TASKalfa MZ4000i/MZ3200i Device Setup Procedure, version 1.0, August 1, 2022
[EOG]	Data Encryption/Overwrite Operation Guide, 3MS2ZSKEDN0, September 2022
[FAX-IG]	FAX System 12 Installation Guide, 303RK5671202, September 2020
[FAX-OG]	FAX System 12 Operation Guide, 2ZSKDENCS500, January 2022
[KMD]	Panther software development <PantherSMB> security software design specification PantherSMB, version 0.20, October 11, 2019, Confidential
[OG]	TASKalfa MZ3200i / MZ4000i Operation Guide, 2ZSKDEN002, May 2022
[VIP]	VaultIP-1XX FW2.2, VaultIP Security Module, Firmware Reference Manual, 007-130220-204, version D, April 6, 2018, INSIDE Secure Proprietary and Confidential Information
[SM]	Service Manual TASKalfa MZ4000i / TASKalfa MZ3200i, AK-740, DF-791 / DF-7120, DP-7140 / DP-7150 / DP-7160 / DP-7170, FAX System 12 / MT-730(B), PF-791 / PF-810, PH-7A / PH-7B / PH-7C / PH-7D, version 5.0, June 2022, Confidential
[TP]	Test Plan – TASKalfa MZ4000i, TASKalfa MZ3200i Series with Hard Disk, FAX System and Data Security Kit, HCD-PP, version 1.0, CAB-23-1388-2663-999, June 13, 2023, Combitech AB

[SER AVA] Single Evaluation Report, Vulnerability Analysis – Kyocera TASKalfa MZ4000i, TASKalfa MZ3200i Series Hard Disk, FAX System and Data Security Kit, HCD-PP, version 1.1, CAB-23-1448-7240-232:001, October 2, 2023, Combitech AB

2 Security Functional Requirement Assurance Activities

This section describes the assurance activities associated with the SFRs defined in the Security Target, [ST], and the results of those activities as performed by the evaluators.

The assurance activities are extracted from the Protection Profile, [PP].

All the test cases that are referred are defined in the test plan, [TP].

2.1 Security Audit (FAU)

The following SFR elements are defined in the ST, [ST]:

- FAU_GEN.1.1
- FAU_GEN.1.2
- FAU_GEN.2.1
- FAU_STG_EXT.1.1

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.1.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its recorded information are consistent with the definition of the SFR.	In [ST] Table 7-5 section 7.6 the auditable events listed in SFR section 6.1.1, Table 6-1 are described with the recorded information (Audit Data) for each event. The start-up and shutdown events stated in FAU_GEN.1.1 a) are also included in the table.

SFR Components	Assurance activity, TSS	Evaluator Assessment
FAU_STG_EXT.1.1	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.	This SFR can be found in [ST] section 7.6 "Audit Log Function" subsection (3). *After the recorded audit log data is temporarily held in the TOE, the log file is transmitted according to the external Audit Log Server set by the U.ADMIN.* *The maximum number of audit log data temporarily stored in the TOE is 2300 logs. When the maximum number of recorded audit log data becomes full, the oldest audit log data is deleted and new audit log data can be stored.*

Table 2, FAU TSS Assurance activities

2.1.2 Guidance, Assurance activities

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	The evaluator shall check the guidance documents to ensure that auditable events and its recorded information are consistent with the definition of the SFRs.	The evaluator found information about auditable events in [EOG] and checked the correspondence with the SFRs defined in [ST].
FAU_STG_EXT.1.1	The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.	The audit log trails are sent by e-mail according to [OG] *Sending the Log History*. Log settings are described in section *History Settings*. The audit log storage settings can be configured in the Web interface and are

SFR Components	Assurance activity, Guidance	Evaluator Assessment
		described in [CCRX] section 10 *Management Settings* under *History Settings* and underlying section 6. The security settings for the IPSec channel are described in [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation.*

Table 3, FAU Guidance assurance activities

2.1.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	The evaluator shall also perform the following tests: The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 1 is appropriately generated. The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods. The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.	**Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FAU_STG_EXT.1.1	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.	**Pass**

Table 4, FAU Test and equivalency assurance activities

2.1.4 KMD, Assurance activities

SFR Components	Assurance activity, KMD	Evaluator Assessment
FAU_GEN.1.1	*No activity*	*NA*
FAU_GEN.1.2		
FAU_GEN.2.1		
FAU_STG_EXT.1.1	*No activity*	*NA*

Table 5, FAU KMD assurance activities

2.2 Cryptographic Support (FCS)

The following SFR elements are defined in the ST, [ST]:

- FCS_CKM.1.1 (a)
- FCS_CKM.1.1 (b)
- FCS_CKM_EXT.4 .1
- FCS_CKM.4
- FCS_COP.1.1(a)
- FCS_COP.1.1(b)
- FCS_RBG_EXT.1.1
- FCS_RBG_EXT.1.2

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.2.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FCS_CKM.1.1 (a)	The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement. Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS. The TSS may refer to the Key Management Description (KMD), described in Appendix F, that may not be made available to the public. TD0642: The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (7). TOE generates RSA-based keys in a manner compliant with NIST SP800-56B in generating asymmetric keys for use in network protection functions. Keys are generates as RSA keys by the TOE and is compatible with 800-56B. TD0642: This Technical Decision makes the SFR less restricted and therefor is ensured even if the SFR is implemented as the HCD-PP describes in the more restricted way.

SFR Components	Assurance activity, TSS	Evaluator Assessment
FCS_CKM.1.1 (b)	The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (8). TOE encrypts communication using 128bit and 256bit AES-CBC as the encryption algorithm used in the network protection function. To generate 128bit and 256bit target encryption keys, random number generation processing according to FCS_RBG_EXT.1 is performed. The TOE uses 128bit and 256bit AES-CBC as the encryption algorithm and keys are generated by the generator defined by FCS_RBG_EXT.1.
FCS_CKM_EXT.4 .1	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.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (9) and section 7.4 “HDD Encryption Function” subsection (4). The TOE stores the session key used by the network protection function in the volatile memory. The data of the volatile memory is erased when the power supply is turned off. The encryption key generated to encrypting HDD is stored in the volatile memory. Therefore, this key is deleted when the TOE is turned off. Also, the key material for generating the encryption key is stored on the main board, but is deleted by performing Data Sanitization function upon TOE disposal. Keying material is stored on main board and erased upon TOE disposal.
FCS_CKM.4	The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed. TD0261: The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.	This SFR can be found in section 7.9 “Network Protection Function” subsection (9) and section 7.4 “HDD Encryption Function” subsection (4). The TOE stores the session key used by the network protection function in the

SFR Components	Assurance activity, TSS	Evaluator Assessment
	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. The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.	volatile memory. The data of the volatile memory is erased when the power supply is turned off. Keys are stored in volatile memory and destroyed when powered off. TD0261: This SFR can be found in section 6.1.2 "*Class FCS: Cryptographic Support*" and subsection "*FCS_CKM.4.1*" where the selection made for destruction, for volatile memory is "powering off a device" and for nonvolatile storage by a "single" overwrite of key data storage location consisting of "a static pattern",
FCS_COP.1.1(a)	*No activity*	*NA*
FCS_COP.1.1(b)	*No activity*	*NA*
FCS_RBG_EXT.1.1 FCS_RBG_EXT.1.2	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.	Section 6.1.2 in [ST]: FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source(s), [assignment: number of hardware-based sources] hardware-based noise source(s)] with a minimum of [selection: 128 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security strength table for hash functions", of the keys and hashes that it will generate. [selection: [assignment: number of software-based sources] software-based noise source(s), [assignment: number of hardware-based sources] hardware-based noise source(s)] with a minimum of [selection: 128 bits, 256 bits] ・[assignment: number of hardware-based sources] hardware-based noise source(s)] with a minimum of [selection: 128 bits, 256 bits] [assignment: number of hardware-based sources] ・8

SFR Components	Assurance activity, TSS	Evaluator Assessment
		[selection: 128 bits, 256 bits] ・256 bit This SFR can be found in section 7.4 "'HDD Encryption Function" and subsection (3). The random number used in this TOE can collect more than 256bits of entropy by inputting Token to Cryptographic Module. The random number generation of Cryptographic Module performs processing using CTR_DRBG in accordance with SP800-90A, and includes 1bit of entropy per 1 bit for random number output. For DRGB random number generation, use the NRGB engine in the Cryptographic Module to set the seed. As the NRBG is configured to generate 1 bit of entropy per 8 'noise' bits and the Conditioning function requires two bits of entropy at its input for each bit of entropy at its output, generating one 256 bits 'full entropy' result requires 256*8*2=4K 'noise' bits. Also, in order to avoid the use of values generated from the same seed, after 256 times 64Kbytes of DRGB random number generation, the automatic generation of random number data by NRGB is executed, and a new value is seeded to the DRGB random number generator by using the random number data. The generator is seeded with 4K noise bits, clearly more than 256bit of entropy. The generator is also replenished with fresh random after 256 times.
FCS_IPSEC_EXT.1.1	*No activity*	*NA* TD0157: This SFR can be found in Section 7.9 "*Network Protection Function*" subsection (12).

SFR Components	Assurance activity, TSS	Evaluator Assessment
	TD0157: The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301. As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.	Keys generated for the IKEv1 exchanges are performed per RFC2409. If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. All keys are held in memory and is only valid with the corresponding SA. Once the SA is terminated the key cannot be used. The TOE can be configured as IPsec security policy database(SPD) to accept or not(Allowed or Denied) communications from networks other than those specified in the IPsec policy. Allowed is set, communication from networks other than those specified in the IPsec rule settings is also accepted. Denied is set, the packet is discarded without accepting communications from networks other than those specified in the IPsec rule settings.
FCS_IPSEC_EXT.1.2	The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). • Encapsulation Settings: Transport mode This is consistent with the information in chapter 6 “Security requirement” section 6.1.13.

SFR Components	Assurance activity, TSS	Evaluator Assessment
FCS_IPSEC_EXT.1.3	The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). The TOE can be configured as IPsec security policy database (SPD) to accept or not communications from networks other than those specified in the IPsec policy. Section 6.1.13 and SFR 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 evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). • Security Protocol: ESP - Cryptographic algorithms: AES-CBC-128, AES-CBC-256 - Authentication algorithms: HMAC-SHA-1, HMAC-SHA-256 Section 6.1.13 and SFR FCS_IPSEC_EXT.1.4: • 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 This is consistent with the description in the TSS.
FCS_IPSEC_EXT.1.5	The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12).

SFR Components	Assurance activity, TSS	Evaluator Assessment
		The evaluator finds that the IKEv1 are being used according to the information in TSS under headline FCS_IPSEC_EXT.1
FCS_IPSEC_EXT.1.6	The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). - IKEv1 algorithms: AES-CBC-128, AES-CBC-256 Section 6.1.13 and SFR FCS_IPSEC_EXT.1.6: The TSF shall ensure the encrypted payload in the *IKEv1* 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*]. • no other algorithm This is consistent with the description in the TSS.
FCS_IPSEC_EXT.1.7	The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.	This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). - IKEv1 mode: Main Mode Section 6.1.13 and SFR FCS_IPSEC_EXT.1.7: The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode. This is consistent with the description in the TSS.
FCS_IPSEC_EXT.1.8	*No activity*	*NA*

SFR Components	Assurance activity, TSS	Evaluator Assessment
FCS_IPSEC_EXT.1.9	The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.	Section 6.1.13 and SFR FCS_IPSEC_EXT.1.9: The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and • no other DH groups This SFR can be found in section 7.9 “Network Protection Function” and subsection (12). Only Oakley Group 14 is used in IKEv1. This is consistent with the description in the TSS.
FCS_IPSEC_EXT.1.10	The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.	Section 6.1.13 and SFR 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. • RSA This SFR can be found in section 7.9 “Network Protection Function” and subsection (7). • Peer Authentication: RSA, Pre-shared Keys This is consistent with the description in the TSS.
FCS_KDF_EXT.1.1	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 SP800-132.	This SFR can be found in section 7.4 “HDD Encryption Function” and subsection (1).

SFR Components	Assurance activity, TSS	Evaluator Assessment
FCS_KYC_EXT.1.1	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.	This SFR can be found in section 7.4 “HDD Encryption Function” and subsection (1). The TOE generates an encryption key for use in encrypting HDD by key derivation function(KDF) in accordance with NIST SP800-108 by using Cryptographic Module. The encryption key size is 256bits. Encryption key is derived from the Salt and IV and KDK. Salt is obtained a RNG generated submask as specified in FCS_RBG_EXT.1 using Cryptographic Module, and KDK uses a unique value for each Hardware. A unique value for each Hardware is stored within Cryptographic Module and cannot be retrieved or rewritten. KDF uses feedback mode and PRF is HMAC-SHA-256(Use SHA-256 in accordance with FCS_COP.1(c)). Encryption algorithms used in KDF are shown in Table 7-4. The key size is specified as 256bits.
FCS_COP.1.1(c)	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.	This SFR can be found in section 7.9 *Network Protection Function* and subsection (12).
FCS_COP.1.1(d)	The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.	This SFR can be found in section 7.4 “HDD Encryption Function” and subsection (2). The key length is specified to 256 bits and the mode is AES-XTS specified in ISO/IEC 18033-3, XTS as specified in IEEE 1619.
FCS_COP.1.1(g)	*No activity*	*NA*
FCS_COP.1.1(h)	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.	This SFR can be found in section 7.4 “HDD Encryption Function” and subsection (1). The HMAC function is specified as HMAC-SHA-256 in Table 7-4.

Table 6, FCS TSS Assurance activities

2.2.2 Guidance, Assurance activities

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FCS_CKM.1.1 (a)	*No activity*	*NA*
FCS_CKM.1.1 (b)	*No activity*	*NA*
FCS_CKM_EXT.4 .1	*No activity*	*NA*
FCS_CKM.4	*No activity* TD0261: 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 and how such situations can be avoided or mitigated if possible. Some examples of what is expected to be in the documentation are provided here. 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, to mitigate this the drive should support the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.	*NA* TD0261: According to [ST] section 7.4 (4): “The encryption key generated to encrypting HDD is stored in the volatile memory. Therefore, this key is deleted when the TOE is turned off. Also, the key material for generating the encryption key is stored on the main board, but is deleted by performing Data Sanitization function upon TOE disposal.” [EOG] section *Disposal* instructs that the HDD/SSD and FAX memory shall be erased before disposal of the machine.

SFR Components	Assurance activity, Guidance	Evaluator Assessment
	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. To reduce this risk, the operating system and file system of the OE should support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion. If a RAID array is being used, only set-ups that support TRIM are utilized. If the drive is connected via PCI-Express, the operating system supports TRIM over that channel. The drive should be healthy and contains minimal corrupted data and should be end of lifed before a significant amount of damage to drive health occurs, this minimizes the risk that small amounts of potentially recoverable data may remain in damaged areas of the drive.	
FCS_COP.1.1(a)	*No activity*	*NA*
FCS_COP.1.1(b)	*No activity*	*NA*
FCS_RBG_EXT.1.1 FCS_RBG_EXT.1.2	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.	No information on random number generation could be found in either [OG], [CCRX] or [EOG]. No guidance information is necessary for the random number generation. There is no configuration to do.
FCS_IPSEC_EXT.1.1	The evaluator shall examine the operational guidance to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for DISCARD, BYPASS and PROTECT.	Information on this subject can be found in [CCRX] section *IPSec Settings*. Restriction can be set to either “Allowed” or “Denied”. “Allowed” specifies that traffic not specified by the IPsec rules is BYPASSed. “Denied” specifies that traffic not specified by the IPsec rules is DISCARDEDed. In both cases, traffic specified by the IPsec rules is PROTECTed.

SFR Components	Assurance activity, Guidance	Evaluator Assessment
	TD0157: The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.	The IPSec rules settings can be done at the web interface, described in [CCRX] section *IPSec Settings.* At the panel IPsec can be turned on or off, described in [OG] 8 *Setup and Registration (System Menu), IPSec* [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies IPSec to be "on" and the restriction to be "Allowed". TD0157: No further actions or information needed.
FCS_IPSEC_EXT.1.2	The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules* and paragraph 1 and 2. [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies Transport mode.
FCS_IPSEC_EXT.1.3	The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.	See FCS_IPSEC_EXT.1.1. All traffic that does not match the IPSec rules is DISCARDed.
FCS_IPSEC_EXT.1.4	The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the algorithms selected by the ST author.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules*. [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies ESP and the following algorithms and modes: - MD5:Disable, - SHA1:Enable, - SHA-256:Enable, - SHA-384:Disable, - SHA-512:Disable, - AES-XCBC:Disable, - AES-GCM-128:Enable, - AES-GCM-192:Disable, - AES-GCM-256:Enable,

SFR Components	Assurance activity, Guidance	Evaluator Assessment
		- AES-GMAC128:Disable, - AES-GMAC-192:Disable, - AES-GMAC-256:Disable
FCS_IPSEC_EXT.1.5	The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test if IKEv2 is selected.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules*. [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies IKEv1.
FCS_IPSEC_EXT.1.6	The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules*. [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies IKEv1 and the following algorithms and modes: - SHA1:Enable, - SHA-256:Enable, - SHA-384:Disable, - SHA-512:Disable - AES-XCBC:Disable.
FCS_IPSEC_EXT.1.7	If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules*. [EOG] section *Changes to IPSec rules after Data Security Kit 10 activation* specifies Main mode.
FCS_IPSEC_EXT.1.8	The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that the values allow for Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no values mandated for the number of packets or number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.	This is configured according to [CCRX] section *IPSec Settings*, subsection *IPSec Rules* (4): “Lifetime (Time): Specifies the lifetime of an ISAKMP SA in seconds.” In [EOG] phase 1 lifetime is specified to 28800 and phase 2 lifetime is specified to 3600 seconds.

<table>
<tr><th>SFR Components</th><th>Assurance activity, Guidance</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td>When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC “A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered.”</td><td></td></tr>
<tr><td>FCS_IPSEC_EXT.1.9</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
<tr><td>FCS_IPSEC_EXT.1.10</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
<tr><td>FCS_KDF_EXT.1.1</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
<tr><td>FCS_KYC_EXT.1.1</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
<tr><td>FCS_COP.1.1(c)</td><td>The evaluator checks the operational guidance documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.</td><td>In [ST] section 6.1.16 FCS_COP.1(c):

<b>FCS_COP.1.1(c) Refinement:</b> The TSF shall perform <b>cryptographic hashing services</b> in accordance with [selection: <i>SHA-1, SHA-256, SHA-384, SHA-512</i>] that meet the following: [<b>ISO/IEC 10118-3:2004</b>].

[selection: <i>SHA-1, SHA-256, SHA-384, SHA-512</i>]
• Listed in Table

<i>Table 6-8 Cryptographic hashing setvices</i>
<table>
<tr><th>Usage</th><th>Hashing services</th></tr>
<tr><td>IPsec IKEv1 Authentication algorithm</td><td>SHA-1,
SHA-256</td></tr>
<tr><td>Key Derivation</td><td>SHA-256</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SFR Components</th><th>Assurance activity, Guidance</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td></td><td><table><tr><td>Signature verification of firmware</td><td>SHA-256</td></tr></table>Only hash for IPsec IKEv1 has multiple choices.
This information can be found in [CCRX] section <i>IPSec Settings</i> under <i>IPsec Rules</i> under paragraph 4 <i>Hash: Selects the hash algorithm.</i> Secure values can be found in [EOG] section <i>Changes to IPSec rules after Data Security Kit 10 activation.</i></td></tr>
<tr><td>FCS_COP.1.1(d)</td><td>If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.</td><td>No multiple choices are supported, according to FCS_COP.1.1(d) in section 6.1.12 in [ST] the only mode/key size is: 256bit AES with XTS mode.
This setup of the encryption is described in [EOG] section <i>After Installation</i>.</td></tr>
<tr><td>FCS_COP.1.1(g)</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
<tr><td>FCS_COP.1.1(h)</td><td><i>No activity</i></td><td><i>NA</i></td></tr>
</table>

Table 7, FCS Guidance assurance activities

2.2.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FCS_CKM.1.1 (a)	The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and “The 186-4 RSA Validation System (RSA2VS)” as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using DSA2VS and RSA2VS according the CAVP#1892 certificate for the cryptographic module used by the TOE.

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	TD0642: The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The 186-4 RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.	TD0642: This Technical Decision makes the SFR less restricted and therefor is ensured even if the SFR is implemented as the HCD-PP describes, in the more restricted way.
FCS_CKM.1.1 (b)	*No activity*	*NA*
FCS_CKM_EXT.4 .1	*No activity*	*NA*
FCS_CKM.4	For each software and firmware key destruction situation the evaluator shall repeat the following tests for Nonvolatile Memory. There is no test for keys in volatile memory, since they are destroyed by powering down the TOE. For the test below, "key" refers to keys and key material. Test 1: The evaluator shall utilize appropriate combinations of specialized Operational Environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are destroyed, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key. For each key subject to destruction, including intermediate copies of keys that are persisted encrypted by the TOE the evaluator shall: 1. Attach to the TOE software/firmware with a debugger, or use alternative methods to perform the tests that follow, including the use of developer-provided special tools that allow inspection of device memory in a special test configuration. 2. Record the value of the key in the TOE subject to destruction. 3. Cause the TOE to perform a normal cryptographic processing with the key from #1. 4. Cause the TOE to destroy the key. 5. Cause the TOE to stop the execution but not exit. 6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file. 7. Search the content of the binary file created in #6 for instances of the known key value from #2. The test succeeds if no copies of the key from #2 are found in step #7 above and fails otherwise.	No keys are stored in non-volatile memory according to [ST] 7.4 HDD Encryption Function (4) and 7.9 Network Protection Function (9); the test is not applicable. TD0261: N/A. Key is held in volatile memory and according to test description "In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary".

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	The evaluator shall perform this test on all keys subject to destruction, including those persisted in encrypted form, to ensure intermediate copies are cleared. TD0261: For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key. Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator 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. Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails. Test 2: Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended. 1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.) 2. Cause the TOE to clear the key. 3. Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.	

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	Test 3: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location: 1. Record the value of the key in the TOE subject to clearing. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1. 3. Cause the TOE to clear the key. 4. Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails. Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location: 1. Record the storage location of the key in the TOE subject to clearing. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1. 3. Cause the TOE to clear the key. 4. Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized. The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.	
FCS_COP.1.1(a)	The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using AESAVS/CMACVS/CCMVS /GCMVS according the CAVP#1892 certificate for the cryptographic module used by the TOE.

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FCS_COP.1.1(b)	The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" RSA2VS as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-4). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using DSA2VS/ECDSA2VS according the CAVP#1892 certificate for the cryptographic module used by the TOE.
FCS_RBG_EXT.1.1	The evaluator shall perform 15 trials for the RBG implementation. If the RBG 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 RBG are valid. If the RBG 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).	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement according the CAVP#1892 certificate for the cryptographic module used by the TOE.
FCS_RBG_EXT.1.2		

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call. The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator. Entropy input: the length of the entropy input value must equal the seed length. Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length. Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied. Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.	
FCS_IPSEC_EXT.1.1	The evaluator uses the operational guidance to configure the TOE to carry out the following tests: 1. The evaluator shall configure the SPD such that there is a rule for DISCARD, BYPASS, PROTECT. The selectors used in the construction of the rule shall be different such that the evaluator can send in three network packets with the appropriate fields in the packet header that each packet will match one of the three rules. The evaluator observes via theaudit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packet was dropped, allowed through without modification, was encrypted by the IPsec implementation. 2. The evaluator shall devise two equal SPD entries with alternate operations – BYPASS and PROTECT. The entries should then be deployed in two	The TOE SPD is only possible to configure through the web and operator panel interfaces which limits the possibilities to perform the tests, [CCRX] section *IPSec Settings*. E.g. when the “Restriction” pararmeter is set to “Allowed”, as stated in [EOG] *Changes to IPSec rules after Data Security Kit 10 activation*, all IP addresses not included in

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	distinct orders and in each case the evaluator shall ensure that the first entry is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation. 3. The evaluator shall repeat the procedure above, except that the two entries should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule. TD0157: The evaluator uses the guidance documentation to configure the TOE to carry out the following tests: a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation. b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.	the ten possible rules are bypassed. **Pass** TD0157: The evaluator configured the TOE to discard, encrypt and bypass packets depending on the packet fields. The encrypt and bypass rules were verified for packets appropriately contructed and all other packets were discarded. **Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FCS_IPSEC_EXT.1.2	The evaluator shall perform the following test(s) based on the selections chosen: 1. (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode. 2. (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.	Only test 2 is applicable since transport mode is used by the TOE, [ST] section 6.1.13, FCS_IPSEC_EXT.1.2 **Pass**
FCS_IPSEC_EXT.1.3	The evaluator shall perform the following test: The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator created entries (there may be a “TOE created” final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE’s interfaces.	**Pass**
FCS_IPSEC_EXT.1.4	The evaluator shall also perform the following tests:	**Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the selected algorithms, and attempt to establish a connection using ESP. The connection should be successfully established for each algorithm.	
FCS_IPSEC_EXT.1.5	(conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.	This test is not applicable since only IKEv1 is used by the TOE, [ST] section 6.1.13, FCS_IPSEC_EXT.1.5.
FCS_IPSEC_EXT.1.6	The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.	**Pass**
FCS_IPSEC_EXT.1.7	The evaluator shall also perform the following test: (conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.	**Pass**
FCS_IPSEC_EXT.1.8	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: 1. (Conditional): The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated. 2. (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance. 3. (Conditional): The evaluator shall perform a test similar to Test 1 for	Test 1 is not applicable since lifetime can only be specified in terms of hours, [ST] section 6.1.13, FCS_IPSEC_EXT.1.8. **Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.	
FCS_IPSEC_EXT.1.9	The evaluator shall also perform the following test (this test may be combined with other tests for this component, for instance, the tests associated with FCS_IPSEC_EXT.1.1): For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.	Only DH group 14 (2048-bit MODP) is applicable according to [ST] section 6.1.13, FCS_IPSEC_EXT.1.9. This is tested in Test Case 2.7, section 3.2.7.
FCS_IPSEC_EXT.1.10	The evaluator shall also perform the following test: For each supported signature algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection.	Not applicable, only RSA is available according to [ST] section 6.1.13, FCS_IPSEC_EXT.1.10.
FCS_KDF_EXT.1.1	*No activity*	*NA*
FCS_KYC_EXT.1.1	*No activity*	*NA*
FCS_COP.1.1(c)	The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode. The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP. <u>Short Messages Test - Bit-oriented Mode</u> The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Short Messages Test - Byte-oriented Mode</u>	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using SHAVS according the CAVP#1892 certificate for the cryptographic module used by the TOE.

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Selected Long Messages Test - Bit-oriented Mode</u> The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Selected Long Messages Test - Byte-oriented Mode</u> The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. <u>Pseudorandomly Generated Messages Test</u> This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.	
FCS_COP.1.1(d)	The following tests are conditional based upon the selections made in the SFR. **AES-CBC Tests** <u>AES-CBC Known Answer Tests</u>	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using AESVS according the CAVP#1933 certificate for the cryptographic module used by the TOE.

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation. **KAT-1.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption. **KAT-2**. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption. **KAT-3**. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].	

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key. **KAT-4**. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128]. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption. <u>AES-CBC Multi-Block Message Test</u> The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation. The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation. <u>AES-CBC Monte Carlo Tests</u> The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:	

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment

	# Input: PT, IV, Key
	for i = 1 to 1000:
	  if i == 1:
	      CT[1] = AES-CBC-Encrypt(Key, IV, PT)
	      PT = IV
	  else:
	      CT[i] = AES-CBC-Encrypt(Key, PT)
	      PT = CT[i-1]
	The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.
	The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.
	AES-GCM Test
	The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:
	128 bit and 256 bit keys
	Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.
	Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.
	Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.
	The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.
	The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.
	The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.	

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	XTS-AES Test The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths: 256 bit (for AES-128) and 512 bit (for AES-256) keys **Three data unit (i.e., plaintext) lengths.** One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller. The evaluator shall test the encrypt functionality using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt. The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally. The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.	
FCS_COP.1.1(g)	The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using HMACVS according the CAVP#1892 certificate for the cryptographic module used by the TOE.
FCS_COP.1.1(h)	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 equal to the result of generating HMAC tags with the same key using a known good implementation.	The NIST FIPS 140-2 Cryptographic Algorithm Verification Program has verified the requirement using HMACVS according the CAVP#1892 certificate for the cryptographic module used by the TOE.

Table 8, FCS Test and equivalency assurance activities

2.2.4 KMD, Assurance activities

SFR Components	Assurance activity, KMD	Evaluator Assessment
FCS_CKM.1.1 (a)	*No activity*	*NA*
FCS_CKM.1.1 (b)	If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)). The KMD is described in Appendix F.	Configuration and get random data function calls as specified in [VIP] 5.5 *TRNG Configuration* and 5.6 *TRNG Get Random Number* are described in [KMD] 5 *Generate random number* including function calls and parameters used. [KMD] 5.2 *Specification, restrictions* specifiy that re-seeding is done every 64k and that AutoSeed is used. The FCS_RBG_EXT description in [ST] 7.4 *HDD Encryption Function (3)* says: As the NRBG is configured to generate 1 bit of entropy per 8 'noise' bits and the Conditioning function requires two bits of entropy at its input for each bit of entropy at its output, generating one 256 bits 'full entropy' result requires 256*8*2=4K 'noise' bits. This is consistent with the key length required by FCS_COP.1(d).
FCS_CKM_EXT.4 .1	The evaluator shall verify the Key Management Description (KMD) includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed. 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 for the destruction.	[ST] 7.4 *HDD Encryption Function* (4) says: The encryption key generated to encrypting HDD is stored in the volatile memory. Therefore, this key is deleted when the TOE is turned off. Also, the key material for generating the encryption key is stored on the main board, but is deleted by performing Data Sanitization function upon TOE disposal. [ST] 7.9 *Network Protection Function* (6) says: TOE stores all pre-shared keys, symmetric keys, and private keys used in the network protection function in NAND or volatile memory. NAND and volatile memory are soldered to the main board, are not removable, and do not provide an interface for all users. In addition,

SFR Components	Assurance activity, KMD	Evaluator Assessment
		data in the volatile memory is erased when the power supply is turned off. [ST] 7.9 *Network Protection Function* (9) says: The TOE stores the session key used by the network protection function in the volatile memory. The data of the volatile memory is erased when the power supply is turned off. This is in accordance with FCS_CKM.4.
FCS_CKM.4	The evaluator shall check to ensure the KMD lists each type of key material, its origin, possible temporary locations (e.g. key register, cache memory, stack, FIFO), and storage location. The evaluator shall verify that the KMD describes when each type of key material is destroyed (for example, on system power off, on wipe function, on disconnection of trusted channels, when no longer needed by the trusted channel per the protocol, etc.). The evaluator shall also verify that, for each type of key and storage, the type of destruction procedure that is performed (cryptographic erase, overwrite with zeros, overwrite with random pattern, or block erase) is listed. If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are destroyed by overwriting once with zeros, while secret keys stored on the internal persistent storage device are destroyed by overwriting three times with a random pattern that is changed before each write"). The evaluator shall check to ensure the KMD lists each type of key material (software-based key storage, BEVs, passwords, etc.) and its origin, storage location, and the method for destruction for each key.	See FCS_CKM_EXT.4. TD0261: See FCS_CKM_EXT.4.

SFR Components	Assurance activity, KMD	Evaluator Assessment
	TD0261: The evaluator examines the KMD 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. The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory, and identifies the memory type (volatile or non-volatile) where key material is stored. The KMD identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.	
FCS_COP.1.1(a)	*No activity*	*NA*
FCS_COP.1.1(b)	*No activity*	*NA*
FCS_RBG_EXT.1.1	*No activity*	*NA*
FCS_RBG_EXT.1.2		
FCS_IPSEC_EXT.1.1	*No activity*	*NA*
FCS_IPSEC_EXT.1.2	*No activity*	*NA*
FCS_IPSEC_EXT.1.3	*No activity*	*NA*
FCS_IPSEC_EXT.1.4	*No activity*	*NA*
FCS_IPSEC_EXT.1.5	*No activity*	*NA*
FCS_IPSEC_EXT.1.6	*No activity*	*NA*
FCS_IPSEC_EXT.1.7	*No activity*	*NA*
FCS_IPSEC_EXT.1.8	*No activity*	*NA*
FCS_IPSEC_EXT.1.9	*No activity*	*NA*

SFR Components	Assurance activity, KMD	Evaluator Assessment
FCS_IPSEC_EXT.1.10	*No activity*	*NA*
FCS_KDF_EXT.1.1	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.	The derivation method is NIST SP 800-108 in feedback mode, [ST] 6.1.17, 7.4 (1). [KMD] 6.2.1 and 6.3.2 describes how the key is derived according to NIST SP800-108 and NIST SP800-56C using the external crypto module. The key is derived at power on. After Deep Sleep the key is reloaded from the VaultIP, [VIP]
FCS_KYC_EXT.1.1	The evaluator shall examine the KMD to ensure that it describes a high level description of the key hierarchy for all accepted BEVs. 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, submask combining, or key encryption. 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. The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.	The TOE generates a symmetric key for HDD en-/decryption. [KMD] section 6.2 describes the procedure, which follows NIST SP800-108, NIST SP800-56C. [ST] section 7.4 (1) also describes the procedure at a high level. The procedure is performed within the external cryptographic module and does not expose any material that might compromise the key. The key size is 256 bits which in this case (AES key) also is the key strength.
FCS_COP.1.1(c)	*No activity*	*NA*
FCS_COP.1.1(d)	*No activity*	*NA*
FCS_COP.1.1(g)	*No activity*	*NA*
FCS_COP.1.1(h)	*No activity*	*NA*

Table 9, FCS KMD assurance activities

2.3 User Data Protection (FDP)

The following SFR elements are defined in the ST, [ST]:

- FDP_ACC.1.1
- FDP_ACF.1.1
- FDP_ACF.1.2
- FDP_ACF.1.3
- FDP_ACF.1.4

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.3.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FDP_ACC.1.1	The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 2 and Table 3.	This SFR can be found in [ST] section 7.2 "Data Access Control Function" and 7.3 "Job Authorization Function" and subsection (1) in both. This information can be found here.
FDP_ACF.1.1		
FDP_ACF.1.2		
FDP_ACF.1.3		
FDP_ACF.1.4		
FDP_DSK_EXT.1.1	The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality. The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.	This SFR can be found in [ST] section 7.4 "HDD Encryption Function" and subsection (2). The evaluator finds that the information is supplied in the [ST] and in the TSS that describes how data is written to the TOE and when encryption is applied.
FDP_DSK_EXT.1.2		

SFR Components	Assurance activity, TSS	Evaluator Assessment
FDP_FXS_EXT.1.1	The evaluator shall check the TSS to ensure that it describes: 1. The fax interface use cases 2. The capabilities of the fax modem and the supported fax protocols 3. The data that is allowed to be sent or received via the fax interface 4. How the TOE can only be used transmitting or receiving User Data using fax protocols	This SFR can be found in [ST] section 7.10 “PSTN Fax-Network Separation” and subsection (1). The evaluator finds in [ST] in chapter 7.10. that the following information can be found. “Fax interface is used to provide fax transmission and fax reception over PSTN. The following protocol is supported is ITU-T G3. Only transmission and reception using the the fax protocol are accepted. Data communication commands from the outside is not accepted.“
FDP_RIP.1.1(a)	The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where image data is stored and how and when it is overwritten.	This SFR can be found in [ST] section 7.5 “Overwrite-Erase Function” and subsection (1). The TOE stores the used image data to be overwritten and erased in the specific area on the HDD and flash memory, and then conducts to overwrite and erase by the process of auditing of the specific area. When receiving an instruction for operation of another basic function and so when waiting for the overwrite-erase function to be performed, or when the existence of the used image data is found because of turning off the power during overwrite-erase processing, the overwrite-erase is conducted by the audit process at the time of coming out of the waiting status or at the time of turning on the power.

Table 10, FDP TSS Assurance activities

2.3.2 Guidance, Assurance activities

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FDP_ACC.1.1		
FDP_ACF.1.1		

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4	The evaluator shall check to ensure that the operational guidance contains a description of the operation to realize the SFP defined in Table 2 and Table 3, which is consistent with the description in the TSS.	No configuration is necessary to achieve the access control rules stated in [ST] table 6-2 and 6-3. The access control mechanisms are verified in [TP] test case 3.1.
FDP_DSK_EXT.1.1 FDP_DSK_EXT.1.2	The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the Device encryption function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient to ensure that all Devices will be encrypted when encryption is enabled or at shipment of the TOE.	Information on activating data encryption can be found in [EOG] *Installing the Security Functions*. The evaluator has followed the steps for test and found the instructions sufficient.
FDP_FXS_EXT.1.1	The evaluator shall check to ensure that the operational guidance contains a description of the fax interface in terms of usage and available features.	The [FAX-IG] describes the physical installation process. [EOG] section *After Installation* describes how to configure fax separation and turn of fax forwarding. [FAX-OG] describes how to operate the fax module, such as preparations before using the fax, sending, receiving fax, etc.
FDP_RIP.1.1(a)	The evaluator shall check to ensure that the operational guidance contains instructions for enabling the Image Overwrite function.	This information can be found in [EOG] section *Security Functions, Overwriting* and *Changing Security Functions, Changing the Data Overwrite Method.* The evaluator has used the instructions during testing and found them sufficient.

Table 11, FDP Guidance assurance activities

2.3.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FDP_ACC.1.1 FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3	The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 2 and Table 3 with each type of interface (e.g., operation panel, Web interfaces) to the TOE. The evaluator testing should include the following viewpoints: • representative sets of the operations against representative sets of the object	**Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FDP_ACF.1.4	types defined in Table 2 and Table 3 (including some cases where operations are either permitted or denied) • representative sets for the combinations of the setting for security attributes that are used in access control	
FDP_DSK_EXT.1.1 FDP_DSK_EXT.1.2	The evaluator shall perform the following tests: Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data. Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material. All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.	**Pass**
FDP_FXS_EXT.1.1	The evaluator shall test to ensure that the fax interface can only be used transmitting or receiving User Data using fax protocols. Testing will be dependent upon how the TOE enforces this requirement. The following tests shall be used and supplemented with additional testing or a rationale as to why the following tests are sufficient: 1. Verify that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. For example, this may be achieved using a terminal application to issue modem commands directly to the TOE from a PC modem (issue terminal command: 'ATDT <TOE Fax Number>') – the TOE should answer the call and disconnect. 2. Verify TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. For example, this may be achieved by using a PC modem to attempt to receive a call from the TOE (submit a fax job from the TOE to <PC modem number>, at PC issue terminal command: 'ATA') – the TOE should disconnect without negotiating a carrier.	**Pass**
FDP_RIP.1.1(a)	The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.	See FMT_SMF.1

Table 12, FDP Test and equivalency assurance activities

2.3.4 KMD, Assurance activities

SFR Components	Assurance activity, KMD	Evaluator Assessment
FDP_ACC.1.1 FDP_ACF.1.1 FDP_ACF.1.2	*No activity*	*NA*

SFR Components	Assurance activity, KMD	Evaluator Assessment
FDP_ACF.1.3		
FDP_ACF.1.4		
FDP_DSK_EXT.1.1 FDP_DSK_EXT.1.2	The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the Device's interface and the Device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine. The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area). The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. If encryption can be enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of confidential data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.	According [ST] section 7.4 (2) the TOE encrypts/decrypts data when storing and reading from the HDD. Image data, job data and TSF data are stored and encrypted on the HDD. The TOE uses the external cryptographic module for the cryptographic operations. The TOE key derivation is described in [KMD] chapter 6 *SATA*, key b and further in [VIP] section 5.12 *Asset Load*. The encryption/decryption operations are described in [VIP] section 5.2 *Encryption.* The boot initialization is described in [KMD] chapter 2 *Library*. Encryption cannot be disabled during operation once enabled.

SFR Components	Assurance activity, KMD	Evaluator Assessment
FDP_FXS_EXT.1.1	*No activity*	*NA*
FDP_RIP.1.1(a)	*No activity*	*NA*

Table 13, FDP KMD Assurance Activities

2.4 Identification and Authentication (FIA)

The following SFR elements are defined in the ST, [ST]:

- FIA_AFL.1.1
- FIA_AFL.1.2
- FIA_ATD.1.1
- FIA_PMG_EXT.1.1
- FIA_UAU.1.1
- FIA_UAU.1.2
- FIA_UAU.7.1
- FIA_UID.1.1
- FIA_UID.1.2
- FIA_USB.1.1
- FIA_USB.1.2
- FIA_USB.1.3

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.4.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FIA_AFL.1.1 FIA_AFL.1.2	The evaluator shall check to ensure that the TSS contains a description of the actions in the case of authentication failure (types of authentication events, the number of unsuccessful authentication attempts, actions to be conducted), which is consistent with the definition of the SFR.	FIA_AFL.1.1 in [ST] section 6.4.1: The TSF shall detect when **an administrator configurable positive integer within 1-10** unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]. • Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from an operational panel. • Consecutive unsuccessful authentication attempts since the last successful authentication occur related to login user name designated by login from a client PC. FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been met, the TSF shall [assignment: *list of actions*]. • Login from the account is locked out between 1 and 60 minutes

SFR Components	Assurance activity, TSS	Evaluator Assessment
		and until the time designated by a device administrator that elapse, or until a device administrator releases lock status. This SFR can be found in section 7.1 “User Management Function” and subsection (1). When the number of consecutive unsuccessful login attempts from the operation panel or a client PC since the last successful authentication, reaches the threshold, the TOE does not allow the users to access to the accounts (i.e. state changes to lockout condition). The number of unsuccessful authentication attempts set by the device administrator can be within 1 to 10 times. After changing to lockout state, If time between 1 and 60 minutes and until the lockout time designated by a device administrator that elapse, or until a device administrator releases lockout state, the TOE is then back to the normal state. This information is consistent with the requirement FIA_AFL.1.
FIA_ATD.1.1	The evaluator shall check to ensure that the TSS contains a description of the user security attributes that the TOE uses to implement the SFR, which is consistent with the definition of the SFR.	FIA_ATD.1.1 ([ST] section 6.1.4): The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*]. • Login User Name, User Authorization, Job Authorization Setting This SFR can be found in section 7.1 “User Management Function” and subsection (2). The TOE defines and maintains user attributes such as login user name, user

SFR Components	Assurance activity, TSS	Evaluator Assessment
		authorization and job authorization setting. This information is consistent with the requirement FIA_ATD.1.
FIA_PMG_EXT.1.1	*No activity*	*NA*
FIA_UAU.1.1	The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers). The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces). The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers. The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.	This SFR can be found in [ST] section 7.1 “User Management Function” and subsection (5). When the user is successfully identified by FIA_UID.1, the TOE verifies if the entered login user password matches with one pre-registered in the TOE. With reception of the device status, the TOE provides information before the user is authenticated. With a list of user jobs and counter information, the TOE displays the information before the user is authenticated. With fax data reception, the TOE receives fax data, before the user is authenticated. List of actions from FIA_UAU.1 section 6.1.4 in [ST]: • Obtain a device status • Display a list of job information • Display counter information • Receive FAX data This list is consistent with FIA_UAU.1. The interfaces used for authentication are described in the beginning of section 7.1.
FIA_UAU.1.2		
FIA_UID.1.1		
FIA_UID.1.2		
FIA_UAU.7.1	The evaluator shall check to ensure that the TSS contains a description of the authentication information feedback provided to users while the authentication is in progress, which is consistent with the definition of the SFR.	FIA_UAU.7 in [ST] section 6.1.4: The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress. • dummy characters（*：asterisk）

SFR Components	Assurance activity, TSS	Evaluator Assessment
		This SFR can be found in section 7.1 “User Management Function” and subsection (6). The TOE displays login user password entered from the operation panel or a client PC on the login screen, which is masked by dummy characters (*: asterisk). This information is consistent with the requirement FIA_UAU.7.
FIA_USB.1.1 FIA_USB.1.2 FIA_USB.1.3	The evaluator shall check to ensure that the TSS contains a description of rules for associating security attributes with the users who succeed identification and authentication, which is consistent with the definition of the SFR.	FIA_USB.1 in [ST] section 6.1.4: **FIA_USB.1.1** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*]. [assignment: *list of user security attributes*] • Login User Name, User Authorization, Job Authorization Setting **FIA_USB.1.2** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*]. [assignment: *rules for the initial association of attributes*] • None **FIA_USB.1.3** The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*]. [assignment: *rules for the changing of attributes*]

SFR Components	Assurance activity, TSS	Evaluator Assessment
		- None This SFR can be found in section 7.1 “User Management Function” and subsection (7). The TOE associates user attributes such as login user name, user authorization and job authorization setting with subjects. This information is consistent with the requirement FIA_USB.1.
FIA_PSK_EXT.1.1 FIA_PSK_EXT.1.2 FIA_PSK_EXT.1.3	The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning. If “bit-based pre-shared keys” is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.	This SFR can be found in [ST] section 7.9 “Network Protection Function” and subsection (12). "Pre-shared Keys: 1-128 length and ASCII charactoers" This includes the required 22 characters in length. “bit-based pre-shared keys” are not selected in FIA_PSK_EXT.1.3.

Table 14, FIA TSS Assurance activities

2.4.2 Guidance, Assurance activities

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FIA_AFL.1.1	The evaluator shall check to ensure that the administrator guidance describes the setting for actions to be taken in the case of authentication failure, if any are defined in the SFR.	In [OG] section *Setting User Login Administration*, *User Account Lockout Setting* can be set to “Lockout Policy”. Followed by three additional settings: “Number of Retries until Locked” (value 1 to 10), “Lockout Duration” (1 to 60 minutes), “Lockout Target” (All or remote login only). [EOG] states that “Lockout Target” shall be set to “All”.
FIA_AFL.1.2		
FIA_ATD.1.1	*No activity*	*NA*
FIA_PMG_EXT.1.1	The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of passwords, and that it provides instructions on setting the minimum password length.	This is described in [OG] section *Setting User Login Administration* and subsection *Password Policy Settings*. [EOG] *After Installation* states the minimum password length to “8 or more characters” but the TOE still have the capability to require 15 characters or greater which is according to the SFR.
FIA_UAU.1.1	The evaluator shall check to ensure that the administrator guidance contains descriptions of identification and authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces), which are consistent with the ST (TSS).	The authentication methods for the interfaces stated in [ST] TSS section 7.1 is described in [OG] chapter 9 *User Authentication and Accounting (User Login, Job Accounting)*. [EOG] *After Installation* states that only local authentication shall be used. The web interface authentication is further described in [CCRX] on section 3 *About Login*.
FIA_UAU.1.2		
FIA_UID.1.1		
FIA_UID.1.2		
FIA_UAU.7.1	*No activity*	*NA*
FIA_USB.1.1	*No activity*	*NA*
FIA_USB.1.2		
FIA_USB.1.3		
FIA_PSK_EXT.1.1		Information on pre-shared keys can be found in [CCRX] section *IPSec Settings*
FIA_PSK_EXT.1.2		

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FIA_PSK_EXT.1.3	The evaluator shall examine the operational guidance to determine that it provides guidance on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.	and sub-section *IPSec Rules* paragraph 3 and 4. [EOG] section *IPsec setting* states that: "Pre-shared key set by the IPsec rule has to be created by using the alphanumeric symbols of 8 digits or more which will not be easily guessed." The evaluator consider this gives guidance on - length – no length shorter than 8 characters is accepted - strength – not easily guessed - allowable characters – alphanumeric symbols, which is a superset of the list contained in FIA_PSK_EXT.1.2.

Table 15, FIA Guidance assurance activities

2.4.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FIA_AFL.1.1 FIA_AFL.1.2	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that the subsequent authentication attempts do not succeed by the behavior according to the actions defined in the SFR when unsuccessful authentication attempts reach the status defined in the SFR. 2. The evaluator shall check to ensure that authentication attempts succeed when conditions to re-enable authentication attempts are defined in the SFR and when the conditions are fulfilled. 3. The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication methods when there are multiple Internal Authentication methods (e.g., password authentication, biometric authentication). 4. The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication attempts.	**Pass**
FIA_ATD.1.1	*No activity*	*NA*
FIA_PMG_EXT.1.1	The evaluator shall also perform the following test:	**Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.	
FIA_UAU.1.1 FIA_UAU.1.2 FIA_UID.1.1 FIA_UID.1.2	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that identification and authentication succeeds, enabling the access to the TOE when using authorized data. 2. The evaluator shall check to ensure that identification and authentication fails, disabling the access to the TOE afterwards when using unauthorized data. The evaluator shall perform the tests described above for each of the authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces).	**Pass**
FIA_UAU.7.1	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication. 2. The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides (e.g., operation panel, identification and authentication via Web interface).	**Pass**
FIA_USB.1.1 FIA_USB.1.2 FIA_USB.1.3	The evaluator shall also perform the following test: The evaluator shall check to ensure that security attributes defined in the SFR are associated with the users who succeed identification and authentication (it is ensured in the tests of FDP_ACF) for each role that the TOE supports (e.g., User and Administrator).	Test Case 3.1 – FDP_ACF.1 Security attribute based access control ensures this.
FIA_PSK_EXT.1.1 FIA_PSK_EXT.1.2 FIA_PSK_EXT.1.3	The evaluator shall also perform the following tests: 1. The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed characters in various combinations that conform to the operational guidance, and demonstrates that a successful protocol negotiation can be performed with each key.	**Pass**

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
	2. [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE. 3. [conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key. 4. [conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.	

Table 16, FIA Test and equivalency assurance activities

2.4.4 KMD, Assurance activities

SFR Components	Assurance activity, KMD	Evaluator Assessment
FIA_AFL.1.1	*No activity*	*NA*
FIA_AFL.1.2		
FIA_ATD.1.1	*No activity*	*NA*
FIA_PMG_EXT.1.1	*No activity*	*NA*
FIA_UAU.1.1	*No activity*	*NA*
FIA_UAU.1.2		
FIA_UID.1.1		
FIA_UID.1.2		
FIA_UAU.7.1	*No activity*	*NA*
FIA_USB.1.1	*No activity*	*NA*
FIA_USB.1.2		
FIA_USB.1.3		
FIA_PSK_EXT.1.1	*No activity*	*NA*

SFR Components	Assurance activity, KMD	Evaluator Assessment
FIA_PSK_EXT.1.2		
FIA_PSK_EXT.1.3		

Table 17, FIA KMD assurance activities

2.5 Security Management (FMT)

The following SFR elements are defined in the ST, [ST]:

- FMT_MOF.1.1
- FMT_MSA.1.1
- FMT_MSA.3.1
- FMT_MSA.3.2
- FMT_MTD.1.1
- FMT_SMF.1.1
- FMT_SMR.1.1
- FMT_SMR.1.2

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.5.1 TSS, Assurance activities

SFR Component	Assurance activity, TSS	Evaluator Assessment
FMT_MOF.1.1	The evaluator shall check to ensure that the TSS contains a description of the management functions that the TOE provides as well as user roles that are permitted to manage the functions, which is consistent with the definition of the SFR. The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.	FTM_MOF.1 in [ST] section 6.1.5: **FMT_MOF.1.1 Refinement:** The TSF shall restrict the ability to *determine the behaviour of* the functions [assignment: *list of functions*] to **U.ADMIN**. [assignment: *list of functions*] • Auditing • User Authentication • Storage Data Encryption • Firmware update • Trusted Commnunication This SFR can be found in section 7.7 “Security Management Function” and subsection (1). TOE allows device administrators only to change setting the following management functions: • Auditing • User Management • Storage Data Encrypiton • Firmware update • Trusted Commnication This information is consistent with the requirement FMT_MOF.1.

<table>
<tr><th>SFR Component</th><th>Assurance activity, TSS</th><th>Evaluator Assessment</th></tr>
<tr>
<td>FMT_MSA.1.1</td>
<td>The evaluator shall check to ensure that the TSS contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.</td>
<td>
<p>FMT_MSA.1 in [ST] section 6.1.5:</p>
<p><b>FMT_MSA.1.1 Refinement:</b> The TSF shall enforce the <b>User Data Access Control SFP in Table 6-2</b> to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i>] the security attributes [assignment: <i>list of security attributes</i>] to [assignment: <i>the authorised identified roles</i>].</p>
<p>[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i>]</p>
<ul><li>Operation(s) as listed in table 6-4</li></ul>
<p>[assignment: <i>list of security attributes</i>]</p>
<ul><li>Security Attributes as listed in table 6-4</li></ul>
<p>[assignment: <i>the authorised identified roles</i>]</p>
<ul><li>Role as listed in table 6-4</li></ul>
<p><i>Table 6-4 Management of security attributes</i></p>
<table>
<tr><th>Security Attributes</th><th>Operation(s)</th><th>Authorised Roles</th></tr>
<tr><td>Box Owner</td><td>modify</td><td>U.ADMINISTRATOR</td></tr>
<tr><td>Box Permission</td><td>modify</td><td>U.ADMINISTRATOR</td></tr>
<tr><td></td><td></td><td>U.NORMAL that matches a Box Owner.</td></tr>
<tr><td>Owner Information</td><td>modify</td><td>U.ADMINISTRATOR</td></tr>
</table>
<p>This SFR can be found in section 7.7 “Security Management Function” and subsection (2).</p>
<p>The TOE allows device administrators only to use box functions for all boxes as shown below.</p>
<ul><li>Read and modify a box owner</li><li>Read and modify a box permission</li></ul>
<p>Whereas, the TOE allows device administrators only to use box functions for documents as shown below.</p>
<ul><li>Read and modify document owner information</li></ul>
</td>
</tr>
</table>

SFR Component	Assurance activity, TSS	Evaluator Assessment
		Normal users are allowed to perform the following operation on the boxes they own. - Read and modify a box permission
FMT_MSA.3.1 FMT_MSA.3.2	The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes which have properties of default values, which are defined in the SFR.	This SFR can be found in [ST] section 7.2 “Data Access Control Function” and subsection (2), and 7.3 “Job Authorization Function” and subsection (2). The TOE sets default values for image data that is initially generated, and a box. Owner information is created using a login user name of the user who initially creates the image data. Box owner is a device administrator who initially creates the box, and the box permission is disabled. Table 7-3 shows that the TOE sets default values for job executable attributes that are targeted functions of job authorization setting on a per user basis. When a user is newly added, default values for executable attributes that are included in job authorization setting, have been set for all jobs. This is consistent with FMT_MSA.3.
FMT_MTD.1.1	*No activity*	*NA*
FMT_SMF.1.1	The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.	In [ST] section 6.1.5: **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*]. [assignment: *list of management functions to be provided by the TSF*] - Functions that manage security attributes (i.e. Box Owner, Box Permission and Owner Information) related to a Box function. - Functions that manage TSF Data (i.e. Login User Name, Login User Password, User Authorization, Job Authorization Settings, Number of Retries until Locked, Lockout Duration, Auto Logout Time Setting, Password Policy Settings, Date and Time Settings, Network encryption Setting, Fax Forward Setting, Send Destination Information for forwarding Audit Log Report)

<table>
<tr><th>SFR Component</th><th>Assurance activity, TSS</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td></td><td>
This SFR can be found in section 7.7 “Security Management Function” and subsection (5).
The TOE provides management function of security attributes for box functions as mentioned in (1), and security management function shown in Table 7-7 and Table 7-8 on TSF data shown in Table 7-7 and Table 7-8.
<i>Table 7-7 Operation of TSF Data by Device Administrators</i>
<table>
<tr><th>TSF Data</th><th>Authorized Operation</th></tr>
<tr><td>Register user information
(Login user name, login user password, user authorization, job authorization settings)</td><td>Edit,
Delete,
Newly create</td></tr>
<tr><td>User account lockout policy settings (number of retries until locked, lockout duration)</td><td>Modify</td></tr>
<tr><td>Lockout list</td><td>Modify</td></tr>
<tr><td>Auto logout time setting</td><td>Modify</td></tr>
<tr><td>Password policy settings</td><td>Modify</td></tr>
<tr><td>Date and time settings</td><td>Modify</td></tr>
<tr><td>Network Encryption Setting</td><td>Modify</td></tr>
<tr><td>FAX forward setting</td><td>Modify</td></tr>
<tr><td>External Audit Log Server transmitting setting</td><td>Modify</td></tr>
</table>
<i>Table 7-8 Operation of TSF Data by Normal Users</i>
<table>
<tr><th>TSF Data</th><th>Authorized Operation</th></tr>
<tr><td>Edit user information
(Login user password associated to the users)</td><td>Edit</td></tr>
</table>
This is consistent.
</td></tr>
<tr><td>FMT_SMR.1.1
FMT_SMR.1.2</td><td>The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.</td><td>FMR_SMR.1 in [ST] section 6.1.5:
FMT_SMR.1.1 Refinement: The TSF shall maintain the roles U.ADMIN, U.NORMAL.
FMT_SMR.1.2 The TSF shall be able to associate users with roles.</td></tr>
</table>

SFR Component	Assurance activity, TSS	Evaluator Assessment
		This SFR can be found in section 7.7 "Security Management Function" and subsection (4). The TOE maintains the user authorizations of device administrators and normal users, and associates users to the user authorizations. This is consistent with FMT_SMR.1.

Table 18, FMT TSS Assurance activities

2.5.2 Guidance, Assurance activities

SFR Component	Assurance activity, Guidance	Evaluator Assessment
FMT_MOF.1.1	The evaluator shall check to ensure that the administrator guidance describes the operation methods for users of the given roles defined in the SFR to operate the management functions.	In [ST] section 6.1.5 in [ST]: **FMT_MOF.1.1 Refinement:** The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN**. [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] • modify the behaviour of [assignment: *list of functions*] • Auditing • User Authentication • Storage Data Encryption • Firmware update • Trusted Commnunication Auditing configuration is described in [OG] section *History Settings* and in [CCRX] 10 *Management Settings*, *History Settings*. Secure values are given in [EOG] section *After Installation*. Information on User Authentication can be found in [OG] chapter 9 *User Authentication and Accounting (User Login, Job Accounting)* and [CCRX] chapter 3 *About Login*, *Local Authentication*. The authentication settings are described in chapter 10 *Management Settings*, section *Authentication*. Secure settings for authentication are described in [EOG] section *After Installation*.

SFR Component	Assurance activity, Guidance	Evaluator Assessment
		Information on Storage Data Encryption can be found in [EOG] sections *Installation* and *Encryption*. Information on Firmware update can be found in [SM] section 5-1 *Firmware update.* Network settings for Trusted Communication can be found in [EOG] section *After Installation*.
FMT_MSA.1.1	The evaluator shall check to ensure that the administrator guidance contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR. The evaluator shall check to ensure that the administrator guidance describes the timing of modified security attributes.	The security attribute rules for document boxes are described in [OG] e.g. *Using Document Boxe*s and in [CCRX] 4 *Document Box.* Secure value for display jobs detail status is described in [EOG] *After installation*.
FMT_MSA.3.1	*No activity*	*NA*
FMT_MSA.3.2		
FMT_MTD.1.1	The evaluator shall check to ensure that the administrator guidance identifies the management operations and authorized roles consistent with the SFR. The evaluator shall check to ensure that the administrator guidance describes how the assignment of roles is managed. The evaluator shall check to ensure that the administrator guidance describes how security attributes are assigned and managed.	Creation, modification, and deletion of users' name and authorizations can only be done by an administrator (U.ADMIN). A user password can be modified by an administrator (U.ADMIN) or the user (U.NORMAL) itself. This is described in [CCRX] sections *Level of Login – Local Authentication* and *Authentication*. The following operations from [ST] FMT_MTD.1, table 6-5, can only be modified by an administrator (U.ADMIN) according to [EOG] section *After Installation*: - Number of Retries until locked, (User Account Lockout Policy Settings) - Lockout Duration, (User Account Lockout Policy Settings) - Lockout List - Auto Logout Time Setting - Password Policy Settings - Date and Time Settings

SFR Component	Assurance activity, Guidance	Evaluator Assessment
	The evaluator shall check to ensure that the administrator guidance describes how the security-related rules (.e.g., access control rules, timeout, number of consecutive logon failures,) are configured.	- Network Encryption Setting - FAX Forward Setting - External Audit Log Server transmitting setting
FMT_SMF.1.1	The evaluator shall check the guidance documents to ensure that management functions are consistent with the assignment in the SFR, and that their operation is described.	The evaluator has checked that the management functions specified in the SFR are described in [OG], [CCRX] and that secure values, where applicable, are specified in [EOG].
FMT_SMR.1.1	*No activity*	*NA*
FMT_SMR.1.2		

Table 19, FMT Guidance assurance activities

2.5.3 Test and Equivalency, Assurance activities

SFR Component	Assurance activity, Test and Equivalency	Evaluator Assessment
FMT_MOF.1.1	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can operate the management functions in accordance with the operation methods specified in the administrator guidance. 2. The evaluator shall check to ensure that the operation results are appropriately reflected. 3. The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.	**Pass**
FMT_MSA.1.1	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to the security attributes in accordance with the operation methods specified in the administrator guidance. 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.	**Pass**

SFR Component	Assurance activity, Test and Equivalency	Evaluator Assessment
	3. The evaluator shall check to ensure that a user that is not part of an authorized role defined in the SFR is not permitted to perform operations on the security attributes.	
FMT_MSA.3.1	If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP_ACF.1.	See FDP_ACF.1.
FMT_MSA.3.2		
FMT_MTD.1.1	The evaluator shall perform the following tests: 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to TSF data in accordance with the operation methods specified in the administrator guidance. 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance. 3. The evaluator shall check to ensure that no users other than users of the given roles defined in the SFR can perform operations to TSF data.	**Pass**
FMT_SMF.1.1	*No activity*	*NA*
FMT_SMR.1.1	As for tests of this SFR, it is performed in the tests of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.	See FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.
FMT_SMR.1.2		

Table 20, FMT Test and equivalency assurance activities

FMT Test and equivalency assurance activities

2.5.4 KMD, Assurance activities

SFR Component	Assurance activity, KMD	Evaluator Assessment
FMT_MOF.1.1	*No activity*	*NA*
FMT_MSA.1.1	*No activity*	*NA*
FMT_MSA.3.1	*No activity*	*NA*
FMT_MSA.3.2		
FMT_MTD.1.1	*No activity*	*NA*
FMT_SMF.1.1	*No activity*	*NA*
FMT_SMR.1.1	*No activity*	*NA*
FMT_SMR.1.2		

Table 21, FMT KMD assurance activities

2.6 Protection of the TSF (FPT)

The following SFR elements are defined in the ST, [ST]:

- FPT_SKP_EXT.1.1
- FPT_STM.1.1
- FPT_TST_EXT.1.1
- FPT_TUD_EXT.1.1
- FPT_TUD_EXT.1.2
- FPT_TUD_EXT.1.3

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.6.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FPT_SKP_EXT.1.1	The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.	This SFR can be found in [ST] section 7.9 “Network Protection Function” and subsection (6). TOE stores all pre-shared keys, symmetric keys, and private keys used in the network protection function in NAND or volatile memory. NAND and volatile memory are soldered to the main board, are not removable, and do not provide an interface for all users. In addition, data in the volatile memory is erased when the power supply is turned off. No special purpose interface for accessing these keys exists.
FPT_STM.1.1	The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.	This SFR can be found in [ST] section 7.6 “Audit Log Function” and subsection (5). The TOE has a system clock inside itself and allows device administrators only to change the time setting of the TOE. The TOE records a date and time of the event with the system clock when auditable events occur. The TOE provides a highly reliable time stamp by recording the time stamps on audit records without delay when the time is recorded by the system clock inside the TOE. Only trusted users (administrators) can set the system clock.
FPT_TST_EXT.1.1	The evaluator shall examine the TSS to ensure that it details the self-tests that	This SFR can be found in [ST] section 7.8 “Trusted operation” and subsection (2). The TOE performs the following self-test at the TOE start-up. • Execution the cryptographic module selftest • Check the integrity of executable module of the security function At the TOE start-up, the TOE performs a self-test of the cryptographic module. In

SFR Components	Assurance activity, TSS	Evaluator Assessment
	are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.	this self-test, a health test of the DRBG and a normal operation test of the encryption function are performed. Also, the TOE also checks the integrity of the executable module of the security function. In case abnormal operation is found by check at the TOE start-up, the users are notified of this abnormal status by displaying it on the Operation Panel of the TOE. If no abnormal item is found on the Operation Panel, the users assume the TOE correctly operates and so the users can use the TOE. This text described the self-test procedures.
FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2 FPT_TUD_EXT.1.3	The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR. The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.	This SFR can be found in [ST] section 7.8 “Trusted operation” and subsection (1). TOE provides administrators with the ability to check firmware versions. The administrator can confirm the firmware version on the device information screen of the operation panel or the web browser. TOE also provides the ability to allow administrators to update firmware. Firmware updates are only possible when the administrator has successfully authenticated the identity and is logged in. When executing the firmware update, TOE verifies firmware data by using signature verification according to FCS_COP.1(b) and hash calculation according to FCS_COP.1(c) from digital signature attached to firmware data. The firmware update processing is executed only when it is determined that there is no problem as a result of the verification. If the verification of the digital signature fails, the TOE displays an error on the operation panel and aborts the update process. This text described the secure update.
FPT_KYP_EXT.1.1	*No activity*	*NA*

Table 22, FPT TSS Assurance activities

2.6.2 Guidance, Assurance activities

SFR Components	Assurance activity, Guidance	Evaluator Assessment
FPT_SKP_EXT.1.1	*No activity*	*NA*
FPT_STM.1.1	The evaluator shall check to ensure that the guidance describes the method of setting the time.	To set the time and date on the panel is described in section [OG] section 8 *Setup and Registration*, *Device Settings*. To set the time and date from the CCRX is described in [CCRX] section 6 *Device settings, Date/Time*. Instruction for an administrator to set the date and time after installation is included in [EOG] *Before Installation*.
FPT_TST_EXT.1.1	The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.	The section *About self-test function* in [EOG] describes what self-tests are performed, how errors are presented and the administrator actions to be performed. The description corresponds to the TSS.
FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2 FPT_TUD_EXT.1.3	The evaluator shall check to ensure that the administrator guidance contains descriptions of the operation methods to obtain the TOE version as well as the operation methods to start update processing, which are consistent with the description of the TSS.	[OG] section *Display for Device Information* describes how to show the model name, serial number, and software version information. The information can be shown on the panel and from the CCRX interface. Firmware update is described in [DevSetup] section *Firmware Update.* Firmware update is only performed by Kyocera service personnel.
FPT_KYP_EXT.1.1	*No activity*	*NA*

Table 23, FPT Guidance assurance activities

2.6.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FPT_SKP_EXT.1.1	*No activity*	*NA*

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FPT_STM.1.1	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance or external network services (e.g., NTP). 2. The evaluator shall check to ensure that the time stamps are appropriately provided.	**Pass**
FPT_TST_EXT.1.1	*No activity*	*NA*
FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2 FPT_TUD_EXT.1.3	The evaluator shall also perform the following tests: 1. The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by means of the operation methods specified by the administrator guidance. 2. The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds using authorized data for updates by means of the operation methods specified by the administrator guidance. 3. The evaluator shall check to ensure that only administrators can implement the application for updates using authorized data for updates. 4. The evaluator shall check to ensure that the updates are correctly performed by obtaining the current version of the TOE after the normal updates finish. 5. The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.)	The TOE is updated by Kyocera service personnel and not by the customer. Step 1 is not applicable. **Pass**
FPT_KYP_EXT.1.1	*No activity*	*NA*

Table 24, FPT Test and equivalency assurance activities

2.6.4 KMD, Assurance activities

SFR Components	Assurance activity, KMD	Evaluator Assessment
FPT_SKP_EXT.1.1	*No activity*	*NA*
FPT_STM.1.1	*No activity*	*NA*
FPT_TST_EXT.1.1	*No activity*	*NA*
FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2 FPT_TUD_EXT.1.3	*No activity*	*NA*

SFR Components	Assurance activity, KMD	Evaluator Assessment
FPT_KYP_EXT.1.1	The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory. The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.	All sensitive data like secure keys, key materialh, IV, digest, MAC and state are stored in an external secure module, [VIP]. [KMD] describes the interface and communication with the secure module in chapter 2 *Library*. The protection of sensitive data inside the secure module is described in [VIP] chapter 3 *Asset Store.*

Table 25, FPT KMD assurance activities

2.7 TOE Access (FTA)

The following SFR elements are defined in the ST, [ST]:

- FTA_SSL.3.1

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.7.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FTA_SSL.3.1	The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.	This SFR can be found in [ST] section 7.1 “User Management Function” and subsection (8). The auto-logout is activated if no operation is performed from the operation panel or a web browser for certain period of time. There are no interactive session exists with the exception of a operation panel and a web browser. • Operation Panel After the user logs on to the TOE and if no operation is performed while the auto-logout time set by the device administrator elapses, the auto-logout is activated. The time can be set to 5 to 495 seconds by the device administrator. • Web browser After the user logs on to the TOE and if no operation is performed for 10 minutes, the auto-logout is activated. This text describes the TSF-initiated termination.

Table 26, FTA TSS Assurance activities

2.7.2 Guidance, Assurance activities

SFR Component	Assurance activity, Guidance	Evaluator Assessment
FTA_SSL.3.1	The evaluator shall check to ensure that the guidance describes the default time interval and, if it is settable, the method of setting the time intervals until the termination of the session.	From [ST] section 6.1.7 in [ST], FTA_SSL.3.1: • Operation Panel: No operation after time set by a device administrator elapsed (between 5 seconds and 495 seconds) • Web browser: No operation after 10 minutes elapsed.

SFR Component	Assurance activity, Guidance	Evaluator Assessment
		The panel session termination for the panel is described in [CCRX] 6 *Device Settings, Energy Saver/Timer* and [EOG] section *After Installation.* It is called *Panel Reset Timer* and the default value is 90 seconds according to [EOG] Appendix. The web browser has a fixed timeout interval of 10 minutes, not possible to change.

Table 27, FTA Guidance assurance activities

2.7.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FTA_SSL.3.1	The evaluator shall also perform the following tests: 1. If it is settable, the evaluator shall check to ensure that the time until the termination of the session can be set up by the method of setting specified in the administrator guidance. 2. The evaluator shall check to ensure that the session terminates after the specified time interval. 3. The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified in the TSS.	The CCRX session terminates after 10 minutes, it cannot be configured. **Pass**

Table 28, FTA Guidance assurance activities

2.7.4 KMD, Assurance activities

SFR Component	Assurance activity, KMD	Evaluator Assessment
FTA_SSL.3.1	*No activity*	*NA*

Table 29, FTA KMD assurance activities

2.8 Trusted Path/Channels (FTP)

The following SFR elements are defined in the ST, [ST]:

- FTP_ITC.1.1
- FTP_ITC.1.2
- FTP_ITC.1.3
- FTP_TRP.1.1 (a)
- FTP_TRP.1.2 (a)
- FTP_TRP.1.3 (a)
- FTP_TRP.1.1 (b)
- FTP_TRP.1.2 (b)
- FTP_TRP.1.3 (b)

Only SFRs components with PP [PP] specific assurance activities are included in the subsections.

2.8.1 TSS, Assurance activities

SFR Components	Assurance activity, TSS	Evaluator Assessment
FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.	FTP_ITC.1 in [ST] section 6.1.8: 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. [selection: IPsec, SSH, TLS, TLS/HTTPS] IPsec [selection: authentication server, [assignment: other capabilities]] [assignment: other capabilities] [assignment: other capabilities] FTP Servr SMTP Server Audi Log Server This SFR can be found in section 7.9 “Network Protection Function” and subsection (10).

<table>
<tr><th>SFR Components</th><th>Assurance activity, TSS</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td></td><td>
<p>When the TOE communicates with each type of servers that are trusted IT products, communication starts between them via a trusted channel. This communication can start from the TOE. The following functions are provided.</p>
<ul>
<li>Scan to send function</li>
<li>Box function (Send Function)</li>
<li>Send to audit log function</li>
</ul>
<p>The TOE provides trusted channel communications listed below.</p>
<p><i>Table 6-4 Trusted channel communications provided by the TOE</i></p>
<table>
<tr><th>Destination</th><th>Protocols</th><th>Encryption algorithm</th></tr>
<tr><td>Mail Server</td><td>IPsec with ESP</td><td>3DES(168 bits), AES(128 bits, 192 bits, 256 bits)</td></tr>
<tr><td>FTP Server</td><td>IPsec with ESP</td><td>3DES(168 bits), AES(128 bits, 192 bits, 256 bits)</td></tr>
<tr><td>Audit log Server</td><td>IPsec with ESP</td><td>3DES(168 bits), AES(128 bits, 192 bits, 256 bits)</td></tr>
</table>
<p>IPsec with ESP is used for Mail Server, FTP Server and Audit log Server. The encryption is either triple-des (168bit key) or AES (128, 192 or 256 bit key).</p>
<p>This text is consistent with FTP_ITC.1.</p>
</td></tr>
</table>

SFR Components	Assurance activity, TSS	Evaluator Assessment
FTP_TRP.1.1 (a) FTP_TRP.1.2 (a) FTP_TRP.1.3 (a)	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.	FTP_TRP.1(a) in [ST] section 6.1.8: 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. [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] IPsec 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. This SFR can be found in section 7.9 “Network Protection Function” and subsection (11). When the TOE communicates with each type of Client PC that are trusted IT products, communication starts between them via a trusted channel. This communication can start from either of the TOE or the trusted IT product. The following functions are provided. • Print function • Operation of a box function from a client PC (web browser) • Operation of security management function from a client PC (web browser) However, use of print function for a direct connection with the TOE is exception. The TOE provides trusted channel communications listed below.

<table>
<tr><th>SFR Components</th><th>Assurance activity, TSS</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td></td><td><i>Table 6-5 Trusted channel communications provided by the TOE</i><table><tr><th>Destination</th><th>Protocols</th><th>Encryption algorithm</th></tr><tr><td>Client PC</td><td>IPsec with ESP</td><td>3DES(168 bits), AES(128 bits, 192 bits, 256 bits)</td></tr></table>
This text is consistent with FTP_TRP.1(a).</td></tr>
<tr><td>FTP_TRP.1.1 (b)
FTP_TRP.1.2 (b)
FTP_TRP.1.3 (b)</td><td>The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-administrative users are indicated, along with how those communications are protected.
The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are consistent with those specified in the requirement, and are included in the requirements in the ST.</td><td>FTP_TRP.1(b) in [ST] section 6.1.8:
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.
[selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS]
IPsec
FTP_TRP.1.2(b) Refinement: The TSF shall permit [selection: the TSF, remote users] to initiate communication via the trusted path.
[selection: the TSF, remote users]
remote users
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.
This SFR can be found in section 7.9 “Network Protection Function” and subsection (11).
When the TOE communicates with each type of Client PC that are trusted IT products, communication starts between them via a trusted channel. This communication can start from either of the TOE or the trusted IT product. The following functions are provided.
• Print function</td></tr>
</table>

<table>
<tr><th>SFR Components</th><th>Assurance activity, TSS</th><th>Evaluator Assessment</th></tr>
<tr><td></td><td></td><td>
<ul>
<li>Operation of a box function from a client PC (web browser)</li>
<li>Operation of security management function from a client PC (web browser)</li>
</ul>
However, use of print function for a direct connection with the TOE is exception.

The TOE provides trusted channel communications listed below.
<i>Table 6-6 Trusted channel communications provided by the TOE</i>
<table>
<tr><th>Destination</th><th>Protocols</th><th>Encryption algorithm</th></tr>
<tr><td>Client PC</td><td>IPsec with ESP</td><td>3DES(168 bits), AES(128 bits, 192 bits, 256 bits)</td></tr>
</table>

This text is consistent with FTP_TRP.1(b).
</td></tr>
</table>

Table 30, FTP TSS Assurance activities

2.8.2 Guidance, Assurance activities

SFR Component	Assurance activity, Guidance	Evaluator Assessment
FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	*No activity*	*NA*
FTP_TRP.1.1 (a) FTP_TRP.1.2 (a) FTP_TRP.1.3 (a)	The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.	Instructions for establishing the remote administrative sessions from the panel can be found in [OG] 8 *Setup and Registration (System Menu), Protocol Settings.* [CCRX] 8 Network Settings describes the same from the CCRX. Secure values for the trusted paths can be found in [EOG] section *After Installation.*
FTP_TRP.1.1 (b) FTP_TRP.1.2 (b) FTP_TRP.1.3 (b)	The evaluator shall confirm that the operational guidance contains instructions for establishing the remote user sessions for each supported method.	Instructions for establishing the remote administrative sessions from the panel can be found in [OG] 8 *Setup and Registration (System Menu), Protocol Settings.* [CCRX] 8 Network Settings describes the same from the CCRX. Secure values for the trusted paths can be found in [EOG] section *After Installation.*

Table 31, FTP Guidance assurance activities

2.8.3 Test and Equivalency, Assurance activities

SFR Components	Assurance activity, Test and Equivalency	Evaluator Assessment
FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	The evaluator shall also perform the following tests: 1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. 2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE. 3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext. 4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected. Further assurance activities are associated with the specific protocols.	IKE/IPsec is the only protocol used for trusted channels. It is used for the e-mail and FTP server communication, [ST] section 7.9. **Pass**
FTP_TRP.1.1 (a) FTP_TRP.1.2 (a) FTP_TRP.1.3 (a)	The evaluator shall also perform the following tests: 1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. 2. For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path. 3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext. Further assurance activities are associated with the specific protocols.	IKE/IPsec is the only protocol used for trusted paths. It is used for administrators' CCRX web server communication, [ST] section 7.9. **Pass**
FTP_TRP.1.1 (b) FTP_TRP.1.2 (b) FTP_TRP.1.3 (b)	The evaluator shall also perform the following tests: 1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote user access method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. 2. For each method of remote access supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote user session without invoking the trusted path. 3. The evaluator shall ensure, for each method of remote user access, the channel data are not sent in plaintext. Further assurance activities are associated with the specific protocols.	IKE/IPsec is the only protocol used for trusted channels. It is used for users' CCRX web server communication [ST] section 7.9. **Pass**

Table 32, FTP Test and equivalency assurance activities

2.8.4 KMD, Assurance activities

SFR Component	Assurance activity, KMD	Evaluator Assessment
FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	*No activity*	*NA*
FTP_TRP.1.1 (a) FTP_TRP.1.2 (a) FTP_TRP.1.3 (a)	*No activity*	*NA*
FTP_TRP.1.1 (b) FTP_TRP.1.2 (b) FTP_TRP.1.3 (b)	*No activity*	*NA*

Table 33, FTP KMD assurance activities

3 Security Assurance Requirement Activities

The sections below specify Evaluation Activities for the Security Assurance Requirements included in the related PP [PP]. The Evaluation Activities are an interpretation of the more general CEM [CEM] assurance requirements. Requirements that not are interpreted are not repeated in detail here.

3.1 ADV, Development

3.1.1 Basic Functional Specification (ADV_FSP.1)

3.1.1.1 Assurance activity

TSS:
The evaluator shall confirm identifiable external interfaces from guidance documents and examine that TSS description identifies all the interfaces required for realizing SFR.
The evaluator shall confirm identification information of the TSFI associated with the SFR described in the TSS and confirm the consistency with the description related to each interface.
The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on identification information of the TSFI in the TSS description as well as on the information of purposes, methods of use, and parameters for each TSFI in the guidance documents.
The assurance activities specific to each SFR are described in Section 4, and also applicable SFRs from Appendix B, Appendix C, and Appendix D, and the evaluator shall perform evaluations by adding to this assurance component.

3.1.1.2 Evaluator assessment

[ADV_2] provides a list of all TSFI and [ADV_1] provides information in section 4.4.

Method of use is described in the relevant detailed use case in section 4.4 [ADV_1]. How the TSFI is invoked, what parameters and the behaviour is well described.

All the TSFIs are mentioned in [ADV_1] section 2.4.1. All TSFI are SFR enforcing. No TSFI are SFR non-interfering, hence, no rationale is needed for the categorisation of such interfaces.

3.2 AGD, Guidance Documentation

3.2.1 Operational User Guide (AGD_OPE.1)

3.2.1.1 Assurance activity

Operational Guidance:
The contents of operational guidance are confirmed by the assurance activities in Section 4, and applicable assurance activities in Appendix B , Appendix C , and Appendix D , and the TOE evaluation in accordance with the CEM.
The evaluator shall check to ensure that the following guidance is provided:
Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

Application note:
During evaluation, the TOE returns to its evaluation configuration. In the field, the TOE may return to the configuration that was in force prior to entering maintenance mode.

3.2.1.2 Evaluator assessment

Security relevant functions described in [OG] can be found in:

- Chapter 8 *Setup and Registration,* specifically in chapter *Network Settings* and *Security Settings*.
- Chapter 9 *User Authentication and Accounting*

Section 9 in [CCRX] described the security settings for the Web interface. Including the Password Policy Settings, User Account Lockout Settings, Data Overwrite Method, SSL settings and Device Certificate settings.

No security relevant modes of operation have been identified.

3.2.2 Preparative Procedures (AGD_PRE.1)

3.2.2.1 Assurance activity

Operational Guidance:
The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

3.2.2.2 Evaluator assessment

The installation is described in section 2 *Installing and Setting up the Machine* in [OG] Section 3 *Preparation before User* describes how to prepare the printer, such as loading the paper.

Section *Additional Preparations for the Administrator* and sub-section *Strengthening the Security* described the security settings required to be set by the System Administrator to assure an secure installation of the TOE.

Secure configuration values are described in [EOG], sections *After Installation* and *Changes to IPSec rules after Data Security Kit 10 activation*.

3.3 ALC, Life-Cycle Support

3.3.1 Labelling of the TOE (ALC_CMC.1)

3.3.1.1 Assurance activity

Operational Guidance:
The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD guidance

and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

3.3.1.2 Evaluator assessment

The Device Information menu at the printers gives information about the firmware versions. The evaluator concludes that the TOE is labeled with its reference and that the system firmware references are consistent with the ST.

3.3.2 TOE CM Coverage (ALC_CMS.1)

3.3.2.1 Assurance activity

Operational Guidance:
The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

3.3.2.2 Evaluator assessment

The TOE is identified in [CIL] as stated in [ST] section 1.2 with name and firmware versions.
The evaluation evidence are identified with document name, version, and date.

The configuration items list, [CIL] incudes specification of the TOE itself in section 2.1, the TOE configuration parts in section 2.2, and all documents comprising the evaluation evidence required at EAL1 in section 2.3.

3.4 ATE, Tests

3.4.1 Independent Testing – Conformance (ATE_IND.1)

3.4.1.1 Assurance activity

Test:
The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP’s Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.
The Test Plan identifies the product models to be tested, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, 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. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in

language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.
The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each model 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) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE.
The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

3.4.1.2 Evaluator assessment

The evaluator test plan is documented in [TP]. In [TP] is test cases defined for all the assurance activities regarding tests defined in [PP] and that are included in [ST].

The independent testing was performed on TASKalfa MZ3200i. The evaluator independent tests were run in a test configuration consistent with the normal user environment described in [ST] section 1.3.2 *TOE Usage*.

The KYOCERA TASKalfa MZ4000i, KYOCERA TASKalfa MZ3200i, KYOCERA TASKalfa M30040i, KYOCERA TASKalfa M30032i, Copystar CS MZ4000i, Copystar CS MZ3200i, TA Triumph-Adler 4063i, TA Triumph-Adler 3263i, UTAX 4063i and UTAX 3263i series execute on the same main board with the same CPU, ARM Cortex-A53 quad 1.6GHz. They are all running the same set of firmware. All other printers listed in [ST] are only different brandings intended for different markets. All models are considered equivalent and it is therefore considered sufficient to test on TASKalfa MZ3200i only.

The TOE was installed and configured as specified in test case 1.1 in [TP]. The installation and configuration followed [OG], [CCRX], and [EOG].

The evaluator documented the test configuration and prerequisites as well as step-by-step test execution descriptions in the test plan [TP]. A summary of the test results is documented in [TP] section 2.7 and all actual results for each test case is documented in chapter 3. All actual results are consistent with the expected test results specified in [TP] chapter 3.

3.5 AVA, Vulnerability Analysis

3.5.1 Vulnerability Survey (AVA_VAN.1)

3.5.1.1 Assurance activity

Test:
As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in printing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report.
For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability.
For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

3.5.1.2 Evaluator assessment

The evaluator has performed a search of public information to determine the vulnerabilities that have been found in certification authority products, the communications and enrollment protocols used, as well as those that pertain to the particular TOE. The public sources National Vulnerability Database, https://nvd.nist.gov/vuln/search, https://cve.mitre.org/cve/, was used for the analysis.

The evaluator has documented the sources consulted and the vulnerabilities found in the report [SER AVA]. For each vulnerability found, the evaluator provides a rationale with respect to its non-applicability.

4 Certificates and Algorithms

This section specify algorithm capabilities for both the certifications claimed by [ST] and which Security Functional Requirements these are mapped to Table 34 and Table 35.

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
AES-CBC • Direction: Decrypt, Encrypt Key Length: 128, 192, 256	FCS_IPSEC_EXT.1: Decrypt, Encrypt AES-CBC-128, AES-CBC-256 FCS_COP.1(a): Decrypt, Encrypt AES-CBC-128, AES-CBC-256
AES-CCM • Key Length: 128, 192, 256 • Tag Length: 64, 80, 96, 112, 128 • IV Length: 56, 64, 72, 80, 88, 96, 104 • Payload Length: 8-256 • AAD Length: 0-256 Prerequisites: C1892 (AES)	---
AES-CMAC ○ Capabilities: ▪ Direction: Generation ▪ Key Length: 128 ▪ MAC Length: 128 ▪ Message Length: 64, 128, 256, 264, 524288 ○ Capabilities: ▪ Direction: Generation ▪ Key Length: 192 ▪ MAC Length: 128 ▪ Message Length: 64, 128, 256, 264, 524288 ○ Capabilities: ▪ Direction: Generation ▪ Key Length: 256 ▪ MAC Length: 128 ▪ Message Length: 64, 128, 256, 264, 524288 ○ Capabilities: ▪ Direction: Verification ▪ Key Length: 128 ▪ MAC Length: 128 ▪ Message Length: 64, 128, 256, 264, 524288 ○ Capabilities: ▪ Direction: Verification ▪ Key Length: 192 ▪ MAC Length: 128 ▪ Message Length: 64, 128, 256, 264, 524288 ○ Capabilities: ▪ Direction: Verification	---

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
- Key Length: 256 - MAC Length: 128 Message Length: 64, 128, 256, 264, 524288	
AES-CTR - Direction: Encrypt Key Length: 128, 192, 256	FCS_RBG_EXT.1: 256 bits
AES-ECB - Direction: Decrypt, Encrypt Key Length: 128, 192, 256	---
AES-KW - Direction: Decrypt, Encrypt - Cipher: Cipher - Key Length: 128, 192, 256 - Payload Length: 128, 192, 256 Prerequisites: C1892 (AES)	---
AES-KWP - Direction: Decrypt, Encrypt - Cipher: Cipher - Key Length: 128, 192, 256 - Payload Length: 296 Prerequisites: C1892 (AES)	---
AES-XTS - Direction: Decrypt, Encrypt - Key Length: 128 - Payload Length: 128, 256, 65536 - Tweak Mode: Hex Prerequisites: C1892 (AES)	---
AES-XTS - Direction: Decrypt, Encrypt - Key Length: 256 - Payload Length: 128, 256, 65536 - Tweak Mode: Hex Prerequisites: C1892 (AES)	---
Counter DRBG	FCS_RBG_EXT.1:

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
• Prediction Resistance: No • Supports Reseed ○ Capabilities: ▪ Mode: AES-256 ▪ Derivation Function Enabled: No ▪ Additional Input: 0 ▪ Entropy Input: 384 ▪ Nonce: 0 ▪ Personalization String Length: 0 ▪ Returned Bits: 128 Prerequisites: C1892 (AES)	Hardware based sources: 8
ECDSA KeyGen (FIPS186-4) • Curve: P-224, P-256, P-384, P-521 • Secret Generation Mode: Extra Bits Prerequisites: C1892 (DRBG)	---
ECDSA KeyVer (FIPS186-4) Curve: P-192, P-224, P-256, P-384, P-521	---
ECDSA SigGen (FIPS186-4) ○ Capabilities: ▪ Curve: P-224 ▪ Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ▪ Curve: P-256 ▪ Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ▪ Curve: P-384 ▪ Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ▪ Curve: P-521 ▪ Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 Prerequisites: C1892 (DRBG), C1892 (SHS)	---
ECDSA SigVer (FIPS186-4) ○ Capabilities: ▪ Curve: P-192 ▪ Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ▪ Curve: P-224 ▪ Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ▪ Curve: P-256	---

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
■ Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ■ Curve: P-384 ■ Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 ○ Capabilities: ■ Curve: P-521 ■ Hash Algorithm: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Prerequisites: C1892 (SHS)	
HMAC-SHA-1 • MAC: 160 • Key sizes < block size • Key size = block size Prerequisites: C1892 (SHS)	FCS_IPSEC_EXT.1, FCS_COP.1(g): Key sizes < block size
HMAC-SHA2-224 • MAC: 224 • Key sizes < block size • Key size = block size Prerequisites: C1892 (SHS)	---
HMAC-SHA2-256 • MAC: 256 • Key sizes < block size • Key size = block size Prerequisites: C1892 (SHS)	FCS_IPSEC_EXT.1, FCS_COP.1(g), FCS_COP.1(h): Key sizes < block size
HMAC-SHA2-384 • MAC: 384 • Key sizes < block size • Key size = block size Prerequisites: C1892 (SHS)	---
HMAC-SHA2-512 • MAC: 512 • Key sizes < block size • Key size = block size Prerequisites: C1892 (SHS)	---
KAS-ECC	---

<table>
<tr><th>Algorithm Capabilities, CAVP Validation Number C1892</th><th>SFRs and operations</th></tr>
<tr><td>
<ul>
<li>Function: Full Public Key Validation, Key Pair Generation, Public Key Regeneration</li>
<li>Scheme:
<ul>
<li>Ephemeral Unified:
<ul>
<li>KAS Role: Initiator, Responder</li>
<li>KDF without Key Confirmation:
<ul>
<li>KDF Option:
<ul><li>ASN.1:</li><li>Concatenation:</li></ul></li>
<li>Parameter Set:
<ul>
<li>EB:
<ul>
<li>Hash Algorithm: SHA2-256</li>
<li>Curve: P-224</li>
<li>MAC Option:
<ul><li>HMAC-SHA2-256:
<ul><li>Key Length: 128</li><li>MAC Length: 64</li></ul></li></ul></li>
</ul></li>
<li>EC:
<ul>
<li>Hash Algorithm: SHA2-256</li>
<li>Curve: P-256</li>
<li>MAC Option:
<ul><li>HMAC-SHA2-384:
<ul><li>Key Length: 192</li><li>MAC Length: 64</li></ul></li></ul></li>
</ul></li>
</ul></li>
</ul></li>
</ul></li>
<li>Full Unified:
<ul>
<li>KAS Role: Initiator, Responder</li>
<li>KDF without Key Confirmation:
<ul>
<li>KDF Option:
<ul><li>ASN.1:</li><li>Concatenation:</li></ul></li>
<li>Parameter Set:
<ul>
<li>EB:
<ul>
<li>Hash Algorithm: SHA2-256</li>
<li>Curve: P-224</li>
<li>MAC Option:
<ul><li>HMAC-SHA2-256:
<ul><li>Key Length: 128</li><li>MAC Length: 64</li></ul></li></ul></li>
</ul></li>
<li>EC:
<ul>
<li>Hash Algorithm: SHA2-256</li>
<li>Curve: P-256</li>
<li>MAC Option:
<ul><li>HMAC-SHA2-384:</li></ul></li>
</ul></li>
</ul></li>
</ul></li>
</ul></li>
</ul></li>
</ul>
</td><td></td></tr>
</table>

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Key Length: 192 ▪ MAC Length: 64 ○ One Pass DH: ▪ KAS Role: Initiator, Responder ▪ KDF without Key Confirmation: ▪ KDF Option: ▪ ASN.1: ▪ Concatenation: ▪ Parameter Set: ▪ EB: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-224 ▪ MAC Option: ▪ HMAC-SHA2-256: ▪ Key Length: 128 ▪ MAC Length: 64 ▪ EC: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-256 ▪ MAC Option: ▪ HMAC-SHA2-384: ▪ Key Length: 192 ▪ MAC Length: 64 ○ One Pass Unified: ▪ KAS Role: Initiator, Responder ▪ KDF without Key Confirmation: ▪ KDF Option: ▪ ASN.1: ▪ Concatenation: ▪ Parameter Set: ▪ EB: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-224 ▪ MAC Option: ▪ HMAC-SHA2-256: ▪ Key Length: 128 ▪ MAC Length: 64 ▪ EC: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-256 ▪ MAC Option: ▪ HMAC-SHA2-384:	

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Key Length: 192 ▪ MAC Length: 64 ○ Static Unified: ▪ KAS Role: Initiator, Responder ▪ KDF without Key Confirmation: ▪ KDF Option: ▪ ASN.1: ▪ Concatenation: ▪ Parameter Set: ▪ EB: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-224 ▪ MAC Option: ▪ HMAC-SHA2-256: ▪ Key Length: 128 ▪ MAC Length: 64 ▪ EC: ▪ Hash Algorithm: SHA2-256 ▪ Curve: P-256 ▪ MAC Option: ▪ HMAC-SHA2-384: ▪ Key Length: 192 ▪ MAC Length: 64 ▪ Derived Keying Material Nonce Types: Random nonce Prerequisites: C1892 (ECDSA), C1892 (SHS), C1892 (DRBG)	
KAS-ECC CDH-Component • Function: Full Public Key Validation, Key Pair Generation, Public Key Regeneration Curve: P-224, P-256, P-384, P-521	---
KDF SP800-108 ○ Capabilities: ▪ KDF Mode: Counter ▪ MAC Mode: CMAC-AES256, HMAC-SHA2-256 ▪ Supported Lengths: 80, 256, 504, 512 ▪ Fixed Data Order: After Fixed Data ▪ Counter Length: 8 ○ Capabilities: ▪ KDF Mode: Feedback ▪ MAC Mode: CMAC-AES256, HMAC-SHA2-256 ▪ Supported Lengths: 80, 256, 504, 512	FCS_KYC_EXT.1, FCS_KDF_EXT.1, FCS_CKM.1(b): Feedback mode, HMAC-SHA2-256, Length 256

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Fixed Data Order: After Fixed Data ▪ Counter Length: 8 ▪ Supports Empty IV Prerequisites: C1892 (DRBG), C1892 (AES), C1892 (HMAC)	
RSA SigGen (FIPS186-4) ○ Capabilities: ▪ Signature Type: PKCS 1.5 ▪ ▪ Properties: ▪ Modulo: 2048 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Properties: ▪ Modulo: 3072 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ○ Capabilities: ▪ Signature Type: PKCSPSS ▪ ▪ Properties: ▪ Modulo: 2048 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384	FPT_TUD_EXT.1, FCS_COP.1(b), FCS_COP.1(c): PKCS 1.5 Modulo 2048 SHA-256

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Salt Length: 384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 512 ▪ Properties: ▪ Modulo: 3072 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 512 Prerequisites: C1892 (SHS)	
RSA SigVer (FIPS186-2) ○ Capabilities: ▪ Signature Type: PKCS 1.5 ▪ ▪ Properties: ▪ Modulo: 1024 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Properties: ▪ Modulo: 1536 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair:	---

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Properties: ▪ Modulo: 2048 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Properties: ▪ Modulo: 3072 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ○ Capabilities: ▪ Signature Type: PKCSPSS ▪ ▪ Properties: ▪ Modulo: 1024 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Salt Length: 0 ▪ Hash Pair:	

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 0 ▪ Properties: ▪ Modulo: 1536 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 0 ▪ Properties: ▪ Modulo: 2048 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 0 ▪ Hash Pair:	

Algorithm Capabilities, CAVP Validation Number C1892	**SFRs and operations**
▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 0 ▪ Properties: ▪ Modulo: 3072 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 0 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 Salt Length: 0	
<u>RSA SigVer (FIPS186-4)</u> ○ Capabilities: ▪ Signature Type: PKCS 1.5 ▪ ▪ Properties: ▪ Modulo: 1024 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Properties: ▪ Modulo: 2048 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Hash Pair:	FPT_TUD_EXT.1, FCS_COP.1(b), FCS_COP.1(c): PKCS 1.5 Modulo 2048 SHA-256

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
■ Hash Algorithm: SHA2-224 ■ Hash Pair: ■ Hash Algorithm: SHA2-256 ■ Hash Pair: ■ Hash Algorithm: SHA2-384 ■ Hash Pair: ■ Hash Algorithm: SHA2-512 ■ Properties: ■ Modulo: 3072 ■ ■ Hash Pair: ■ Hash Algorithm: SHA-1 ■ Hash Pair: ■ Hash Algorithm: SHA2-224 ■ Hash Pair: ■ Hash Algorithm: SHA2-256 ■ Hash Pair: ■ Hash Algorithm: SHA2-384 ■ Hash Pair: ■ Hash Algorithm: SHA2-512 ○ Capabilities: ■ Signature Type: PKCSPSS ■ ■ Properties: ■ Modulo: 1024 ■ ■ Hash Pair: ■ Hash Algorithm: SHA-1 ■ Salt Length: 160 ■ Hash Pair: ■ Hash Algorithm: SHA2-224 ■ Salt Length: 224 ■ Hash Pair: ■ Hash Algorithm: SHA2-256 ■ Salt Length: 256 ■ Hash Pair: ■ Hash Algorithm: SHA2-384 ■ Salt Length: 384 ■ Hash Pair: ■ Hash Algorithm: SHA2-512 ■ Salt Length: 496 ■ Properties: ■ Modulo: 2048 ■ ■ Hash Pair:	

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
▪ Hash Algorithm: SHA-1 ▪ Salt Length: 160 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 512 ▪ Properties: ▪ Modulo: 3072 ▪ ▪ Hash Pair: ▪ Hash Algorithm: SHA-1 ▪ Salt Length: 160 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-224 ▪ Salt Length: 224 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-256 ▪ Salt Length: 256 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-384 ▪ Salt Length: 384 ▪ Hash Pair: ▪ Hash Algorithm: SHA2-512 ▪ Salt Length: 512 • Public Exponent Mode: Random Prerequisites: C1892 (SHS)	
SHA-1 Message Length: 0-51200 Increment 8	FIA_PSK_EXT.1, FCS_IPSEC_EXT.1, FCS_COP.1(g)
SHA2-224 Message Length: 0-51200 Increment 8	---
SHA2-256 Message Length: 0-51200 Increment 8	FIA_PSK_EXT.1, FCS_IPSEC_EXT.1, FCS_COP.1(g), FCS_COP.1(h), FCS_COP.1(c)

Algorithm Capabilities, CAVP Validation Number C1892	SFRs and operations
SHA2-384 Message Length: 0-102400 Increment 8	---
SHA2-512 Message Length: 0-102400 Increment 8	---

Table 34, Kyocera MFP Cryptographic Module(A), CAVP Validation Number C1892, hardware version 2.1.10.

Algorithm Capabilities, CAVP Validation Number C1933	SFR
AES-ECB • Direction: Decrypt, Encrypt Key Length: 128, 256	---
AES-XTS • Direction: Decrypt, Encrypt • Key Length: 128 • Payload Length: 128, 256, 65536 • Tweak Mode: Number Prerequisites: C1933 (AES)	---
AES-XTS • Direction: Decrypt, Encrypt • Key Length: 256 • Payload Length: 128, 256, 65536 • Tweak Mode: Number Prerequisites: C1933 (AES)	FDP_DSK_EXT.1, FCS_COP.1(d): Decrypt, Encrypt Payload length: 128

Table 35, Kyocera MFP Cryptographic Module(A) – FDE, CAVP Validation Number C1933, hardware version 2.3.

5 References

[CCpart1]	Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, version 3.1, revision 5, April 2017, CCMB-2017-04-001
[CCpart2]	Common Criteria for Information Technology Security Systems, Part 2: Security functional components, version 3.1, revision 5, April 2017, CCMB-2017-04-002
[CCpart3]	Common Criteria for Information Technology Security Systems, Part 3: Security assurance components, version 3.1, revision 5, April 2017, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version 3.1, revision 5, April 2017, CCMB-2017-04-004
[HCD-PP]	Protection Profile for Hardcopy Device, IPA, NIAP, and the MFP Technical Community, Version 1.0, September 10, 2015 Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017
[STAFS]	2020:1, Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om ackreditering
[KM]	Kvalitetsmanual IS, utgåva 3.4, CAB-132499, Combitech AB

See section 1.1 for the referred evaluation evidences.

6 Abbreviations and Glossary

CC	Common Criteria
FER	Final Evaluation Report
HCD	Hardcopy Device (eg. printer)
KMD	Key Management Description
MFP	Multi-function printer
NIAP	National Information Assurance Partnership
PP	Protection Profile
SAR	Security Assurance Requirements
SER	Single Evaluation Report
SFR	Security Functional Requirements
TOE	Target of Evaluation
TSF	TOE Security Functions

Further explanation on the above abbreviations can be found in [CCpart1].

Appendix A – Security Functional Requirements Table

Legend:

R = Required
C = Conditionally Mandatory
O = Optional
S = Selection
U = an SFR that plays a supporting role to other SFRs

Objective: **SFR:**	**O.ACCESS_CONTROL**	**O.ADMIN_ROLES**	**O.AUDIT**	**O.COMMS_PROTECTION**	**O.FAX_NET_SEPATATION**	**O.IMAGE_OVERWRITE**	**O.KEY_MATERIAL**	**O.PURGE_DATA**	**O.STORAGE_ENCRYPTION**	**O.TSF_SELF_TEST**	**O.UPDATE_VERIFICATION**	**O.USER_AUTHORIZATION**	**O.USER_I&A**
FAU_GEN.1			**R**										
FAU_GEN.2			**R**										
FAU_SAR.1			**O**										
FAU_SAR.2			**O**										
FAU_STG.1			**O**										
FAU_STG.4			**O**										
FAU_STG_EXT.1			**R**										
FCS_CKM.1(a)				**R**									
FCS_CKM.1(b)				**R**					**S**				
FCS_CKM.4				**U**				**O**	**U**				
FCS_CKM_EXT.4				**U**				**O**	**U**				
FCS_COP.1(a)				**R**									
FCS_COP.1(b)				**S**							**S**		
FCS_COP.1(c)									**U**		**S**		
FCS_COP.1(d)									**U**				
FCS_COP.1(e)									**U**				
FCS_COP.1(f)									**U**				
FCS_COP.1(g)				**S**									
FCS_COP.1(h)									**O**				

Objective: **SFR:**	**O.ACCESS_CONTROL**	**O.ADMIN_ROLES**	**O.AUDIT**	**O.COMMS_PROTECTION**	**O.FAX_NET_SEPATATION**	**O.IMAGE_OVERWRITE**	**O.KEY_MATERIAL**	**O.PURGE_DATA**	**O.STORAGE_ENCRYPTION**	**O.TSF_SELF_TEST**	**O.UPDATE_VERIFICATION**	**O.USER_AUTHORIZATION**	**O.USER_I&A**
FCS_COP.1(i)									**U**				
FCS_HTTPS_EXT.1				**S**									
FCS_IPSEC_EXT.1				**S**									
FCS_KDF_EXT.1									**O**				
FCS_KYC_EXT.1									**C**				
FCS_PCC_EXT.1									**O**				
FCS_RBG_EXT.1				**U**					**U**				
FCS_SMC_EXT.1									**S**				
FCS_SNI_EXT.1									**S**				
FCS_SSH_EXT.1				**S**									
FCS_TLS_EXT.1				**S**									
FDP_ACC.1	**R**											**R**	
FDP_ACF.1	**R**											**R**	
FDP_DSK_EXT.1									**C**				
FDP_FXS_EXT.1					**C**								
FDP_RIP.1(a)						**O**							
FDP_RIP.1(b)								**O**					
FIA_AFL.1													**U**
FIA_ATD.1												**U**	
FIA_PMG_EXT.1													**R**
FIA_PSK_EXT.1				**S**									
FIA_UAU.1													**R**
FIA_UAU.7													**R**
FIA_UID.1		**U**											**R**
FIA_USB.1													**R**
FMT_MOF.1		**R**											
FMT_MSA.1	**U**											**R**	

Objective:	**O.ACCESS_CONTROL**	**O.ADMIN_ROLES**	**O.AUDIT**	**O.COMMS_PROTECTION**	**O.FAX_NET_SEPATATION**	**O.IMAGE_OVERWRITE**	**O.KEY_MATERIAL**	**O.PURGE_DATA**	**O.STORAGE_ENCRYPTION**	**O.TSF_SELF_TEST**	**O.UPDATE_VERIFICATION**	**O.USER_AUTHORIZATION**	**O.USER_I&A**
SFR:													
FMT_MSA.3	**U**											**R**	
FMT_MTD.1	**U**												
FMT_SMF.1	**U**	**R**										**R**	
FMT_SMR.1	**U**	**R**										**R**	
FPT_KYP_EXT.1							**C**						
FPT_SKP_EXT.1				**R**									
FPT_STM.1			**U**										
FPT_TST_EXT.1										**R**			
FPT_TUD_EXT.1											**R**		
FTA_SSL.3													**R**
FTP_ITC.1			**U**	**R**									
FTP_TRP.1(a)				**R**									
FTP_TRP.1(b)				**R**									

Table 36, Security functional requirements table