Xerox® AltaLink™ EC8036 & EC8056

Assurance Activity Report

Version 1.2

June 2022

Document prepared by

www.lightshipsec.com

Table of Contents

1 Introduction

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

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Evaluation Facility	Lightship Security USA
Developer/Sponsor	Xerox Corporation
TOE	Xerox® AltaLink™ EC8036 & EC8056 Software Version: 103.023.031.35105
Security Target	Xerox® AltaLink™ EC8036 & EC8056 Security Target, v1.4
Protection Profile	Protection Profile for Hardcopy Devices, v1.0, September 10, 2015
	Protection Profile for Hardcopy Devices, v1.0, Errata #1

1.2 Evaluation Methods

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

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1R5
Evaluation Methodology	CEM v3.1R5
Supporting Documents	N/A
Interpretations	**HCD v1.0** TD0074 FCS_CKM.1(a) Requirement in HCD PP v1.0 *This TD is applicable as FCS_CKM.1 is claimed for the TOE.* TD0157 FCS_IPSEC_EXT.1.1 - Testing SPDs *This TD is applicable as IPSec is claimed for the TOE.* TD0176 FDP_DSK_EXT.1.2 - SED Testing *This TD is not applicable as SED drives are not in scope.* TD0219 NIAP Endorsement of Errata for HCD PP v1.0 (Errata #1, June 2017)

	This TD is applicable to the TOE and the Errata is included in the Test Plan.
	TD0253 Assurance Activities for Key Transport *This TD is not applicable to the TOE as Key Transport under FCS_COP.1(i) is not claimed.*
	TD0261 Destruction of CSPs in flash *This TD applies to the TOE.*
	TD0299 Update to FCS_CKM.4 Assurance Activities *This TD applies to the TOE and supersedes TD0261.*
	TD0393 Require FTP_TRP.1(b) only for printing *This TD applies to the TOE.*
	TD0474 Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 *This TD applies to the TOE.*
	TD0494 Removal of Mandatory SSH Ciphersuite for HCD *This TD applies to the TOE.*
	TD0562 Test Activity for Public Key Algorithms *This TD applies to the TOE.*

2 TOE Details

2.1 Overview

The TOE is a hardcopy device that copies and prints with scan and fax capabilities, commonly known as Multi-Function Device (MFD), Multi-Function Printer (MFP) or simply printer. The TOE is deployed within office environments for general copy/print/scan/fax use by non-administrative users.

2.2 TOE Models

1 The TOE includes the models listed in the table below. The TOE models vary in print speeds.

Table 3: TOE models

Model	Software Version	CPU / OS
AltaLink™ EC8036	103.023.031.35105	Intel Atom E3845 Wind River Linux 6.0 (Linux 3.10 32-bit)
AltaLink™ EC8056		

2.3 Reference Documents

Table 4: List of Reference Documents

Ref	Document
[ST]	Xerox® AltaLink™ EC8036 & EC8056 Security Target, v1.3
[SIG]	Secure Installation and Operation of your Xerox® EC8036/EC8056 Color Multifunction Printer v1.2
[SAG]	Xerox® EC8036/EC8056 Color Multifunction Printer System Administrator Guide, v1.0
[AGD]	Xerox® EC8036/EC8056 Color Multifunction Printer User Guide, v1.0
[AGD-1]	Xerox® AltaLink® Series Smart Card Installation and Configuration Guide, v3.0
[KMD]	Xerox®AltaLink™EC8036 & EC8056 Key Management Description v1.5
[Entropy]	Xerox® AltaLink™ Printers Entropy Description March 2022, v1.1
[DTR]	Xerox® AltaLink™ EC8036 & EC8056 HCD 1.0 Detailed Test Report, v1.1 Xerox® AltaLink™ EC8036 & EC8056 HCD 1.0 Test Evidence, v1.1

2.4 Summary of SFRs

Table 5: List of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
FCS_CKM.1(a)	Cryptographic Key Generation (for asymmetric keys)
FCS_CKM.1(b)	Cryptographic Key Generation (Symmetric keys)
FCS_CKM.4(a)	Cryptographic Key Destruction
FCS_CKM_EXT.4	Extended: Cryptographic Key Material Destruction
FCS_COP.1(a)	Cryptographic Operation (Symmetric Encryption/Decryption)
FCS_COP.1(b)	Cryptographic Operation (for Signature Generation and Verification)
FCS_COP.1(c)	Cryptographic operation (Hash Algorithm)
FCS_COP.1(d)	Cryptographic operation (AES Data Encryption/Decryption)
FCS_COP.1(g)	Cryptographic Operation (for Keyed-hash message authentication)
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FCS_IPSEC_EXT.1	Extended: IPsec selected
FCS_HTTPS_EXT.1	Extended: HTTPS selected
FCS_KYC_EXT.1	Extended: Key Chaining
FCS_TLS_EXT.1	Extended: TLS selected
FCS_SSH_EXT.1	Extended: SSH selected
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security attribute based access control
FDP_DSK_EXT.1	Extended: Protection of Data on Disk
FDP_FXS_EXT.1	Extended: Fax separation
FDP_RIP.1(a)	Subset residual information protection
FDP_RIP.1(b)	Subset residual information protection
FIA_AFL.1	Authentication Failure Handling

Requirement	Title
FIA_ATD.1	User attribute definition
FIA_PMG_EXT.1	Extended Password Management
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_KYP_EXT.1	Extended: Protection of Key and Key Material
FPT_SKP_EXT.1	Extended: Protection of TSF Data
FPT_STM.1	Reliable Time Stamps
FPT_TST_EXT.1	Extended: TSF testing
FPT_TUD_EXT.1	Extended: Trusted update
FTA_SSL.3	TSF-initiated Termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1(a)	Trusted Path (for Administrators)
FTP_TRP.1(b)	Trusted Path (for Non-administrators)

3 Evaluation Activities for SFRs

3.1 Security Audit (FAU)

3.1.1 FAU_GEN.1Audit data generation

3.1.1.1 TSS

3.1.1.2

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.

Findings:	ST Section 6.2.1 describes audit generation, references the table in the SFR for the list of auditable events, and identifies recorded audit information to include a timestamp, type of event, subject identity (where applicable) and outcome of event. The auditable events and recorded information are consistent with the SFR.

3.1.1.3 Operational Guidance

3 The evaluator shall check the guidance documents to ensure that auditable events and its recorded information are consistent with the definition of the SFRs.

Findings:	The SIG in the Section ‘Audit Log’ describes the audit logs and the information captured in the audit log; the recorded information is consistent with the SFR.

3.1.1.4 Test

4 The evaluator shall also perform the following tests:

5 The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 1 is appropriately generated.

6 The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods.

7 The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.

Findings:	The evaluator for the DTR test case FAU_GEN.1 performs actions to generate the baseline audit events identified in Table 1 and confirms that the required audit events are generated. For the FIA_UAU.1 auditable events, the evaluator ensures that the test for FIA_UAU.1 exercises all the I&A mechanisms claimed in the TSS and verifies that audit events are generated for all use of the I&A mechanisms.

3.1.2 FAU_GEN.2 User identity association

8 The Assurance Activities for FAU_GEN.1 address this SFR.

3.1.3 FAU_STG_EXT.1 Extended: External Audit Trail Storage

3.1.3.1 TSS

9 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.

Findings:	ST Section 6.2.2 — The TSS describes that using EWS the TOE can be configured to transfer audit logs to a designated file server in the operational environment. Audit log transfer can be configured for scheduled daily transmission or a 'send now' option will transfer the audit logs immediately. Audit logs are transferred via SFTP only. The TSS in ST Section 6.8.4 describes the SSH trusted channel used for audit transfer.

10 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.

Findings:	ST Section 6.2.3 — The TSS describes that the TOE will store a maximum of 15,000 audit log entries and will overwrite oldest events first if the maximum is reached. When local audit storage reaches 90% capacity, an email is sent to the administrator. Access to the audit log is restricted to authorized administrators. The SIG Section 'Audit Log' describes that audit records can be configured to be pushed to an external server daily. Details on how to transfer audit logs to an external server can be found in section 4 subsection "audit log" of the SAG document.

3.1.3.2 Operational Guidance

11 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.

Findings:	The SIG Section 'SFTP Filing' describes how to configure the trusted channel for audit transfer.

3.1.3.3 Test

12 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.

Findings:	The evaluator for the DTR test case for FAU_STG_EXT.1 follows the guidance to configure the SSH/SFTP trusted channel and performs an audit log transfer using Wireshark to capture the traffic. The evaluator confirms that the audit transfer is successful. The evaluator then examined the Wireshark capture to confirm that the traffic is encrypted during the transfer. The software used for the audit transfer test is identified in the DTR.

3.1.4 FAU_STG.1 Protected audit trail storage

3.1.4.1 TSS

13 The evaluator shall check to ensure that the TSS contains a description of the means of preventing audit records from unauthorized access (modification, deletion).

Findings:	ST Section 6.2.3 describes that EWS and the Control Panel are used to access the audit logs. The system administrator is the only user with authorized access to the audit log.

3.1.4.2 Operational Guidance

14 The evaluator shall check to ensure that the TSS and operational guidance contain descriptions of the interfaces to access the audit records, and if the descriptions of the means of preventing audit records from unauthorized access (modification, deletion) are consistent.

Findings:	The SIG Section 'Audit Log' describes how the system administrator downloads the audit log and protocol logs for review, and that the logs are not accessible to non-admin users.

3.1.4.3 Test

15 The evaluator shall also perform the following tests:

16 1. The evaluator shall test that an authorized user can access the audit records.

17 2. The evaluator shall test that a user without authorization for the audit data cannot access the audit records.

Findings:	The evaluator for the DTR test for FAU_STG.1 configures the audit settings and shows that only the admin users can see the settings to access the audit records, and that the non-admin user cannot see the settings.

3.1.5 FAU_STG.4 Prevention of audit data loss

3.1.5.1 TSS

18 The evaluator shall check to ensure that the TSS contains a description of the processing performed when the capacity of audit records becomes full, which is consistent with the definition of the SFR.

Findings:	ST Section 6.2.3 describes that the TOE will overwrite the oldest audit records when storage becomes full. When audit storage capacity reaches 90% an email warning is sent to the administrator; subsequent warning emails are sent to the administrator every time the maximum of 15,000 records has been reached until audit log storage is clear.

3.1.5.2 Operational Guidance

19 The evaluator shall check to ensure that the operational guidance contains a description of the processing performed (such as informing the authorized users) when the capacity of audit records becomes full.

Findings:	The SIG Section ‘Audit Log’ describes the audit log processing for sending a warning email to the administrator when the log is at 90% full and every time it reaches max capacity at 15,000 entries.

3.1.5.3 Tests

20 The evaluator shall also perform the following tests:

21 1. The evaluator generates auditable events after the capacity of audit records becomes full by generating auditable events in accordance with the operational guidance.

22 2. The evaluator shall check to ensure that the processing defined in the SFR is appropriately performed to audit records.

Findings:	The evaluator for the DTR test for FAU_STG.4 runs a script to rapidly fill the audit log with 13500 records and demonstrates that an email alert is sent when the log reached 90% full.

3.2 Cryptographic Support (FCS)

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

3.2.1.1 TSS

23 *(Modified by NIAP TD0074)*

24 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.

25 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.

26 The TSS may refer to the Key Management Description (KMD), described in Appendix F, that may not be made available to the public.

Findings:	ST Section 6.6.1 describes how the TOE complies with the 800-56A and 800-56b and identifies the relevant sections in the standard which include sections on key establishment. The TSS does not identify any TOE-specific extensions not described in the NIST publication or any alternative implementation.

3.2.1.2 Test

27 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.

Note:	This test AA is addressed with CAVP certificates DSA 1140, RSA 2296, ECDSA 994.

3.2.2 FCS_CKM.1(b) Cryptographic Key Generation (symmetric keys)

3.2.2.1 TSS

28 The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

Findings:	ST Section 6.6.1 — The TSS describes how the TOE invokes the CTR-DRBG by reference to the proprietary Entropy Assessment Report which contains the detailed description.

3.2.2.2 KMD

29 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)).

30 The KMD is described in Appendix F.

Findings:	The KMD in Section 1.3 describes the TOE incorporates its own DRBG seeded with 256-bits of entropy. The TSS in Section 6.6.1 indicates that the TOE uses CTR-DRBG for encryption/decryption using AES in CBC mode and key size of 256 bits.

3.2.3 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

3.2.3.1 TSS

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

Findings:	ST Section 6.6.1 — Table 17 in the TSS lists all key and key materials along with description of how each key is stored, how it is protected (where applicable), when the key is no longer needed, how and when the key is expected to be destroyed.

3.2.3.2 KMD

32 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.

Findings:	The table in Chapter 22 of the KMD identifies the keys and key materials used by the TOE and describes where they reside, and when they are no longer needed.

33 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.

Findings:	The table in Chapter 22 of the KMD includes a key lifecycle. The table list all keys and key material, how they are used, where they reside, end-of-life, and destruction method. Chapter 3 of the KMD includes a detailed description of key destruction.

3.2.4 FCS_CKM.4(a) Cryptographic key destruction

(Modified by NIAP TD0261 and TD0299)

3.2.4.1 TSS

34 The evaluator shall verify the TSS provides a high-level description of how keys and key material are destroyed.

35 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.

36 The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

Findings:	ST Section 6.6.1 — the TSS describes that keys and key material in volatile memory are destroyed by removal of power to the memory; in non-volatile memory, keys are overwritten with a single overwrite of the values (0x35 or 0x97). The TSS also indicates that there are no known configurations or circumstances that do not conform to the key destruction requirement.

3.2.4.2 KMD

37 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.

Findings:	The 'Derivation/usage' column of the table in Chapter 22 of the KMD describes how the keys stored in volatile memory are derived and used; the column labeled 'End-of-Life' describes that they are destroyed at power-off.

38 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.

Findings:	Chapter 22 in the KMD lists each type of key stored in the TOE and identifies the memory type where key material is stored. The table identifies which keys are stored in the BIOS NVM SPI Flash Memory, in the unencrypted/encrypted file system or in RAM.

39 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.

Findings:	The KMD Chapter 21 describes the two interfaces that are used to service commands to read/write memory. The KMD description supports the selections in the SFR.

3.2.4.3 Operational Guidance

40 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.

41 Some examples of what is expected to be in the documentation are provided here.

42 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.

43 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.

44 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.

Findings:	The SIG ‘Additional items’ on page 22 states that there are no situations where key destruction may be delayed at the physical layer.

3.2.4.4 Test

45 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.

46 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:

47 1. Record the value of the key in the TOE subject to clearing.

48 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

49 3. Cause the TOE to clear the key.

50 4. Cause the TOE to stop the execution but not exit.

51 5. Cause the TOE to dump the entire memory of the TOE into a binary file.

52 6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.

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

54 Test 2: Applied to each key held in non-volatile memory and subject to destruction by the TOE, except for replacing a key using the selection [*a new value of a key of the same size*]. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

55 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.)

56 2. Cause the TOE to clear the key.

57 3. Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.

58 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:

59 1. Record the value of the key in the TOE subject to clearing.

60 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

61 3. Cause the TOE to clear the key.

62 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.

63 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:

64 1. Record the storage location of the key in the TOE subject to clearing.

65 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

66 3. Cause the TOE to clear the key.

67 4. Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.

68 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.

Findings:	The evaluator for the DTR test case FCS_CKM.4 performs all steps defined for test 2, test 3 and test 4 to delete each of the keys that are stored in non-volatile memory per the ST Table 17. Keys stored in non-volatile memory are destroyed by overwrite with a value of (0x35 or 0x97), so after performing the key destructions, the evaluator searched for both values and confirmed that the search returned the (0x97) value. The evaluator also verified that the destroyed keys no longer exist in the TOE. Test 1 does not apply to the TOE because the keys in volatile memory are only destroyed

	via a removal of power to the TOE. This is consistent with the claims made in FCS_CKM.4(a).

3.2.5 FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

3.2.5.1 Test

69 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.

Note:	The test assurance activity for FCS_COP.1(a) is covered by the CAVP certificates AES 3451, AES 4265.

3.2.6 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

3.2.6.1 Tests

70 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.

Note:	The test assurance activity for FCS_COP.1(b) is covered by CAVP certificates RSA 2690, RSA 2296, ECDSA 698.

3.2.7 FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

3.2.7.1.1 TSS

71 The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Findings:	ST Section 6.6.4 – The TSS describes cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512 that are used for TLS, IPsec, SSH, Storage encryption and trusted update (signature verification).

3.2.7.1.2 Operational Guidance

72 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.

Findings:	The SIG Section ‘FIPS 140-2 Mode’ and Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ include instructions for configuring the hash sizes.

3.2.7.1.3 Test

73 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.

74 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.

75 Short Messages Test - Bit-oriented Mode

76 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.

77 Short Messages Test - Byte-oriented Mode

78 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.

79 Selected Long Messages Test - Bit-oriented Mode

80 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 $1 \le i \le m$. For SHA-512, the length of the i-th message is 1024 + 99*i, where $1 \le i \le m$. 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.

81 Selected Long Messages Test - Byte-oriented Mode

82 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 $1 \le i \le m/8$. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where $1 \le i \le m/8$. 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.

83 Pseudorandomly Generated Messages Test

84 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.

Note:	The test assurance activity for FCS_COP.1(c) is addressed by CAVP # SHS 2847, SHS 3511.

3.2.8 FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

3.2.8.1 TSS

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

Findings:	The TSS in ST Section 6.6.2 – describes key sizes and mode used for encryption.

3.2.8.2 Operational Guidance

86 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.

Findings:	The SIG Section 'Data Encryption' indicates that the encryption mode and key size are set by default and no additional cryptographic settings are configurable in the TOE for data encryption.

3.2.8.3 Test

87 The following tests are conditional based upon the selections made in the SFR.

88 **AES-CBC Tests**

89 <u>AES-CBC Known Answer Tests</u>

90 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.

91 **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.

92 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.

93 **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.

94 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.

95 **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].

96 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.

97 **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].

98 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.

99 AES-CBC Multi-Block Message Test

100 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.

101 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.

102 AES-CBC Monte Carlo Tests

103 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:

104 # Input: PT, IV, Key

105 for i = 1 to 1000:

106 if i == 1:

107 CT[1] = AES-CBC-Encrypt(Key, IV, PT)

108 PT = IV

109 else:

110 CT[i] = AES-CBC-Encrypt(Key, PT)

111 PT = CT[i-1]

112 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.

113 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.

114 AES-GCM Test

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

116 128 bit and 256 bit keys

117 **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.

118 **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.

119 **Two IV lengths.** If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

120 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.

121 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.

122 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.

123 XTS-AES Test

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

125 256 bit (for AES-128) and 512 bit (for AES-256) keys

126 **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 2^{16} bits, whichever is smaller.

127 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.

128 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.

129 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.

Note:	The test assurance activity for FCS_COP.1(d) is covered by CAVP AES #3451 and AES #4265.

3.2.9 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

3.2.9.1.1 Test

130 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.

Note:	The test assurance activity for FCS_COP.1(g) is covered by CAVP HMAC #2197 and HMAC #2810

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

3.2.10.1 TSS

131 For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Findings:	The TSS in ST Section 6.6.1 describes that the TOE implements random bit generation services using CTR_DRBG (AES) seeded with at least 256-bits of entropy from a hardware noise source. This statement is consistent with the selection in FCS_RBG_EXT.1.2 and can also be found in the Entropy Description.

3.2.10.2 Entropy Description

132 The evaluator shall ensure the Entropy Description provides all of the required information as described in Appendix E. The evaluator assesses the information provided and ensures the TOE is providing sufficient entropy when it is generating a Random Bit String.

Findings:	The Entropy Description provides all required information and has been approved for this evaluation.

3.2.10.3 Operational Guidance

133 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.

Findings:	The SIG Section 'FIPS 140-2 Mode' includes a statement that DRBG selection is not configurable in the TOE.

3.2.10.4 Test

134 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.

135 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).

136 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.

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

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

139 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.

140 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.

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

Note:	The test assurance activity for FCS_RBG_EXT.1 is covered by CAVP DRBG #845 and DRBG #1336.

3.2.11 FCS_IPSEC_EXT.1 Extended: IPsec selected

3.2.11.1 FCS_IPSEC_EXT.1.1

(Modified by NIAP TD0157)

3.2.11.1.1 TSS

142 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.

143 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.

Findings:	Section 6.8.5 in the TSS – The TOE implements an SPD that describes the rules for processing inbound and outbound packets. The TSS description of rule processing for inbound and outbound traffic covers both the initial packets and packets that are part of an established SA.

3.2.11.1.2 Operational Guidance

144 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.

Findings:	The SIG Section ‘IPsec’ provides the instructions for configuring the SPD rules for packets processing and cover all 3 cases and the ordering of rules. The SIG details are consistent with the TSS and the evaluator followed these instructions to configure the SPD for testing.

3.2.11.1.3 Test

145 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.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.1 configured the IPsec settings to create several new rules and new host groups, then the evaluator sent traffic to the TOE to verify that the SPD rules are applied.

3.2.11.2 FCS_IPSEC_EXT.1.2

3.2.11.2.1 TSS

146 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).

Findings:	Section 6.8.5 in the TSS — Both transport mode and tunnel mode are supported in the evaluated configuration.

3.2.11.2.2 Operational Guidance

147 The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

Findings:	The SIG in Section ‘IPsec’ describes the IPsec settings configurable in the TOE including the settings for tunnel or transport mode.

3.2.11.2.3 Test

148 The evaluator shall perform the following test(s) based on the selections chosen:

149 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.

150 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.

Findings:	The DTR test case for FCS_IPSEC_EXT.1.2 configured the TOE IPsec settings to operate in tunnel mode with the cryptographic parameters identified in the SFR, and also configured a test VM to operate in tunnel mode. The evaluator initiated a connection to the TOE and used Wireshark to capture the traffic. The evaluator then examined the pcap file to verify that the connection is successful in tunnel mode. The evaluator then changed the IPsec setting to operate in transport mode and verified successful connections using transport mode.

3.2.11.3 FCS_IPSEC_EXT.1.3

3.2.11.3.1 TSS

151 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.

Findings:	ST Section 6.8.5 — The TSS describes that packets are processed against the SPD. If no rules are found to match an existing SPD, the default action is to bypass (pass through) the packet. A final rule is configured to discard.

3.2.11.3.2 Operational Guidance

152 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.

Findings:	The SIG in the Section titled ‘IPsec’ provides instructions on how to construct the SPD. In order to PROTECT traffic, a policy needs to be made on the TOE and any traffic matching the policy will be protected through the tunnel. In order to BYPASS traffic, a policy rule must be created to allow “all” traffic after original policy rules for protect and traffic that matches said policy will bypass the tunnel. In order to DISCARD traffic, a policy rule must be created to block all protocol groups for the tunnel.

3.2.11.3.3 Test

153 The evaluator shall perform the following test:

154 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.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.3 sends traffic to the TOE to match the bypass rules and traffic that does not match any of the SPD rules, and verifies that the SPD rules are applied accordingly.

3.2.11.4 FCS_IPSEC_EXT.1.4

3.2.11.4.1 TSS

155 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).

Findings:	ST Section 6.8.5 — The TSS description lists AES-CBC-128 and AES-CBC-256 and the same HMAC algorithms identified in FCS_COP.1(g).

3.2.11.4.2 Operational Guidance

156 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.

Findings:	The SIG Section 'IPsec' describes the IPsec settings that are configurable in the TOE.

3.2.11.4.3 Test

157 The evaluator shall also perform the following tests:

158 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.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.4 configures the IPsec settings and shows that connection using ESP is successfully established for each of the algorithms identified in the TSS.

3.2.11.5 FCS_IPSEC_EXT.1.5

3.2.11.5.1 TSS

159 The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

Findings:	ST Section 6.8.5 — The TSS states that the TOE implements IKEv1.

3.2.11.5.2 Operational Guidance

160 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.

Findings:	The SIG Section 'IPsec' includes instructions for configuring the IPsec settings. IKEv1 is configured by default.

3.2.11.5.3 Test

161 (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.

Findings:	Test not applicable. The TOE does not claim IKEv2.

3.2.11.6 FCS_IPSEC_EXT.1.6

3.2.11.6.1 TSS

162 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.

Findings:	In Section 6.8.5 of the ST — The TSS description covers that the TOE uses AES-CBC-128, AES-CBC-256 for encrypting the IKEv1 payload.

3.2.11.6.2 Operational Guidance

163 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.

Findings:	The SIG Section ‘IPsec’ describes the configurable settings for the configuring the mandated algorithms.

3.2.11.6.3 Test

164 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.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.6 configures the mandated algorithm and sends encrypted traffic. The evaluator used Wireshark to capture the traffic and then reviewed the captured files to confirm the algorithm that was used in the negotiation.

3.2.11.7 FCS_IPSEC_EXT.1.7

3.2.11.7.1 TSS

165 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.

Findings:	ST Section 6.8.5 — The TSS description includes a statement that only main mode is supported for IKEv1 Phase 1 exchanges. Aggressive mode is not supported.

3.2.11.7.2 Operational Guidance

166 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.

Findings:	The SIG Section 'IPsec' describes the IPsec settings configurable in the TOE. The mode is not configurable in the TOE; it is set by default.

3.2.11.7.3 Test

167 The evaluator shall also perform the following test:

168 (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.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.7 configures the IPsec settings described in the SIG. Using Wireshark to capture the traffic, the evaluator sends IPsec traffic to the TOE using aggressive mode and shows that the connection is not established in aggressive mode. The evaluator then reset the IPsec peer to send traffic to the TOE using IPsec in main mode and showed that the connection is successful.

3.2.11.8 FCS_IPSEC_EXT.1.8

3.2.11.8.1 Operational Guidance

169 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.

170 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."

Findings:	The SIG Section 'IPsec' describes the IPsec settings for configuring the SA lifetimes for IKEv1. The Section contains instructions for configuring the SA. Time-based limits are supported and allow for Phase 1 SA values of 24 hours and 8 hours for Phase 2 SAs. The evaluator followed the SIG instructions for configuring the SA lifetimes during testing.

3.2.11.8.2 Test

171 Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

172 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.

173 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.

174 3. (Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.8 configures the SA lifetimes for IKEv1 phase 1 and phase 2, then sends IPsec traffic to the TOE while using Wireshark to capture the traffic; the test demonstrates that the configured SA lifetimes are applied. Test 1 is not applicable to the TOE because there is no option to configure SA lifetimes based on the number of bytes.

3.2.11.9 FCS_IPSEC_EXT.1.9

3.2.11.9.1 TSS

175 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.

Findings:	TSS in ST Section 6.8.5 identifies DH group 14 only as does the SFR.

3.2.11.9.2 Test

176 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):

177 For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.

Findings:	The evaluator for the DTR test case FCS_IPSEC_EXT.1.9 configures the IPsec DH group settings, then sends traffic to the TOE using Wireshark to capture the traffic. The evaluator verifies that the connection is successful using the only supported DH group.

3.2.11.10 FCS_IPSEC_EXT.1.10

3.2.11.10.1 TSS

178 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.

Findings:	ST Section 6.8.5 — The TSS contains a description of the IKE peer authentication process which uses RSA algorithm as well as pre-shared keys.

3.2.11.10.2 Test

179 The evaluator shall also perform the following test:

180 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.

Findings:	The DTR test for FCS_IPSEC_EXT.1.10 sends traffic to the TOE using each supported signature algorithm; the test uses Wireshark to capture the traffic. The evaluator reviews the Wireshark capture to verify that peer authentication is successful with each supported algorithm and a successful connection is established.

3.2.12 FCS_HTTPS_EXT.1 Extended: HTTPS selected

3.2.12.1.1 TSS

181 The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack.

Findings:	ST Section 6.8.2 — The TSS describes that the TOE provides the EWS interface for remote administration and this interface is accessed via TLS/HTTPS. The TOE does not support client authentication.

3.2.12.1.2 Test

182 Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

3.2.13 FCS_KYC_EXT.1 Extended: Key Chaining

3.2.13.1 TSS

183 The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

Findings:	ST Section 6.7.2 – The TOE generates a 256-bit BEV for disk encryption.

3.2.13.2 KMD

184 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.

Findings:	KMD Chapter 10 provides the details of the key chain. The TOE uses a submask as the DEK. The BEV and all key materials are stored encrypted

185 The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could

be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

Findings:	KMD Chapter 10 describes how the key chain process functions and includes a diagram of the key hierarchy. The key hierarchy shows no point where the chain could be broken; the effective strength of the BEV is maintained throughout the Key Chain.

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

Findings:	KMD Chapter 10 states the generated BEV is 256-bits and the chain is extended with a SHA-256 hash.

3.2.14 FCS_TLS_EXT.1 Extended: TLS selected

(Modified by NIAP TD0474)

3.2.14.1 TSS

187 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

Findings:	ST Section 6.8.3 describes that the TOE implements TLS 1.2 and lists supported ciphersuites that are identical to the listing in the SFR. The SIG Section 'Transport Layer Security (TLS)' describes the configuration settings for TLS and includes instructions for configuring TLS to conform to the description in the TSS. The SIG description also lists the ciphersuites supported by the TOE and the list is identical to the list in the SFR.

3.2.14.2 Test

188 The evaluator shall also perform the following test:

189 1. The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

190 2. The evaluator shall setup a man-in-the-middle tool between the TOE and the TLS Peer and shall perform the following modifications to the traffic:

191 a) [Conditional: TOE is a server] Modify ~~at least one~~ a byte in the ~~server's nonce in the Server Hello~~ data of the client's Finished handshake message, and verify that the server ~~denies the client's Finished handshake message~~ rejects the connection and does not send any application data.

192 b) [Conditional: TOE is a client] Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.

193 c) [Conditional: TOE is a client] If a DHE or ECDHE ciphersuite is supported, modify the signature block in the Server's KeyExchange handshake message, and verify that the client rejects the connection after receiving the Server KeyExchange.

194 d) [Conditional: TOE is a client] Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.

Findings:	The evaluator for the DTR test case FCS_TLS_EXT.1 uses the Greenlight Tool to show that the TOE can establish TLS connections using all the ciphersuites listed in the SFR. The evaluator uses Greenlight to setup man-in-the-middle attacks both where the TOE is a client and where the TOE is a server and uses Wireshark to capture the traffic and show the handshake failures required by the test assurance activity.

3.2.15 FCS_SSH_EXT.1 Extended: SSH selected

3.2.15.1 FCS_SSH_EXT.1.1

None

3.2.15.2 FCS_SSH_EXT.1.2

3.2.15.2.1 TSS

195 The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.5, and ensure that password-based authentication methods are also allowed.

Findings:	ST Section 6.8.4 identifies the supported public key algorithms SSH_RSA. Password-based authentication methods are also allowed. All public key algorithms supported by the TOE are found in FCS_SSH_EXT.1.5.

3.2.15.2.2 Test

196 The evaluator shall also perform the following tests:

197 1. The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.

198 2. Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.

Findings:	The evaluator for the DTR test case FCS_SSH_EXT.1.2 uses instructions in the SIG to configure SSH and connects to the SSH/SFTP server using password and using public key. The test demonstrates successful connections using the public key algorithms in the SFR.

3.2.15.3 FCS_SSH_EXT.1.3

3.2.15.3.1 Test

199 The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

Findings:	The evaluator for the DTR test case FCS_SSH_EXT.1.3 setup Wireshark to monitor SSH traffic, and uses the Greenlight server tool to send large packets to the TOE to demonstrate that packets larger than 40,000 bytes are dropped.

3.2.15.4 FCS_SSH_EXT.1.4

3.2.15.4.1 TSS

200 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

Findings:	ST Section 6.8.4 — The TSS description indicates that the TOE uses an SSH client for SSH/SFTP transfer of audit logs to a remote log server. This description does not specify optional characteristics and the identified encryption algorithms are identical to those identified in the SFR. Note – SIG Section 'SFTP Filing' includes a statement that the SSH encryption algorithms are not configurable in the TOE.

3.2.15.4.2 Test

201 The evaluator shall also perform the following test:

202 The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

Findings:	The evaluator for the DTR test case for FCS_SSH_EXT.1.4 setups Wireshark to monitor SSH traffic and uses the Greenlight tool to establish successful SSH connections using the encryption algorithms defined in the SFR.

3.2.15.5 FCS_SSH_EXT.1.5

(Modified per NIAP TD0562)

3.2.15.5.1 TSS

203 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

Findings:	TSS in ST Section 6.8.4 describes the TOE implementation of the SSH protocol including the supported public key algorithms. The public key algorithms specified in

	the TSS are identical to those listed in the component. The SIG in the Section titled 'SFTP Filing' indicates that the SSF settings are not configurable in the TOE.

3.2.15.5.2 Test

204 The evaluator shall also perform the following test:

205 The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

Findings:	The evaluator for the DTR test for FCS_SSH_EXT.1.5 setups Wireshark to monitor SSH traffic and uses the Greenlight tool to demonstrate successful SSH connections using the public key algorithms defined by the SFR.

3.2.15.6 FCS_SSH_EXT.1.6

3.2.15.6.1 TSS

206 The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component. The evaluator shall also check the operational guidance to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).

Findings:	TSS in ST Section 6.8.4 – data integrity algorithms used for SSH connections are hmac-sha1, hmac-sha1-96, hmac-sha2-512. This list is consistent with the integrity algorithms claimed in FCS_SSH_EXT.1.6. The SIG Section 'SFTP Filing' indicates that SSH parameters are not configurable in the TOE.

3.2.15.6.2 Test

207 The evaluator shall also perform the following test:

208 The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

Findings:	The evaluator for the DTR test case FCS_SSH_EXT.1.6 setup Wireshark to monitor SSH traffic and uses the Greenlight tool to demonstrate successful SSH connections using the data integrity algorithms defined by the SFR.

3.2.15.7 FCS_SSH_EXT.1.7

209 *(Modified per NIAP TD0494)*

3.2.15.7.1 Operational Guidance

210 The evaluator shall check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

Findings:	The SIG Section 'SFTP Filing' includes a statement that the SSH cryptographic algorithms are not configurable in the TOE.

3.2.15.7.2 Test

211 The evaluator shall also perform the following test:

212 1. [Conditional: TOE is a client] The evaluator shall configure an SSH server to permit all allowed key exchange methods. For each allowed key exchange method, the evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt succeeds.

213 2. [Conditional: TOE is a server] The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.

214 3. [Conditional: TOE is a server] For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.

Findings:	The DTR test for FCS_SSH_EXT.1.7 setups Wireshark to monitor SSH traffic and uses the Greenlight tool to demonstrate successful SSH connections using the allowed key exchange methods specified by the SFR. Test 2 and test 3 are not applicable as the TOE is an SSH client.

3.3 User Data Protection (FDP)

3.3.1 FDP_ACC.1 Subset access control

215 It is covered by assurance activities for FDP_ACF.1.

3.3.2 FDP_ACF.1 Security attribute based access control

3.3.2.1 TSS

216 The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 2 and Table 3.

Findings:	ST Section 6.3.2 provides a high-level description of the access control algorithm including Condition 1 and Notes 1 through 4.

3.3.2.2 Operational Guidance

217 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.

Findings:	The SIG Section ‘Authorization’ describes the configurable settings to realise the SFP.

3.3.2.3 Test

218 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.

219 The evaluator testing should include the following viewpoints:

- representative sets of the operations against representative sets of the object 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

Findings:	The evaluator for the DTR test case FDP_ACF_EXT.1 creates users with different role privileges and creates a subset of the objects covered by the SFP, and then demonstrates that the access control SFP is enforced.

3.3.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

3.3.3.1 TSS (Modified by NIAP TD0176)

220 If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The tester shall confirm that the specific SED is listed in the TSS, documented and verified to be CC certified against the FDE EE cPP.

Findings:	N/A - This option was not selected.

221 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.

Findings:	The TSS in ST Section 6.7.1 provides a comprehensive description of how data is written to the device by the file system code and encrypted by a block i/o driver.

222 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.

Findings:	N/A – The TOE includes two cryptographic modules: Mocana and OpenSSL that it uses for cryptographic operations.

223 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.

Findings:	TSS Section 6.7.1 – Encryption is enabled by default. The description lists areas of the device that are not encrypted.

3.3.3.2 Operational Guidance

224 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.

Findings:	SIG Section ‘Data Encryption’ describes that encryption is enabled by default. There is no additional setup to enable encryption.

3.3.3.3 KMD

225 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.

Findings:	The KMD Chapter 10 describes the data encryption engine and provides details of its implementation. The description includes a diagram showing the main components within the data path.

226 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).

Findings:	The KMD includes a statement that encryption is enabled by default. Chapter 10 describes the data flow and identifies the unencrypted disk partitions.

227 The evaluator shall verify 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.

Findings:	The KMD Chapter 10 describes the boot initialization process. Encryption is enabled by default.

3.3.3.4 Test

228 The evaluator shall perform the following tests:

229 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.

230 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.

231 All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.

Findings:	The evaluator for the DTR test case FDP_DSK_EXT.1 first identifies the location where user documents and confidential TSF data are stored, verifies that they are stored encrypted, and verifies that they can be decrypted with the correct keys.

3.3.4 FDP_FXS_EXT.1 Extended: Fax separation

3.3.4.1 TSS

232 The evaluator shall check the TSS to ensure that it describes:

233 1. The fax interface use cases

234 2. The capabilities of the fax modem and the supported fax protocols

235 3. The data that is allowed to be sent or received via the fax interface

236 4. How the TOE can only be used transmitting or receiving User Data using fax protocols

Findings:	The TSS in ST Section 6.9.1 describes the Fax interface, how it is used, the supported fax protocols, what data can be transmitted via the fax interface, and how the TOE prevents interconnection between the PSTN and the internal network.

3.3.4.2 Operational Guidance

237 The evaluator shall check to ensure that the operational guidance contains a description of the fax interface in terms of usage and available features.

Findings:	The SIG Section 'Embedded Fax' describes the settings for the fax interface.

3.3.4.3 Test

238 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:

239 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.

240 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.

Findings:	The evaluator for the DTR test case FDP_FXS_EXT.1 setup the fax on the TOE device and used an advance phone line simulator and Tera Term VT to show that incoming and outgoing calls using fax carrier protocols are accepted and those using data carriers are rejected.

3.3.5 FDP_RIP.1(a) Subset residual information protection

3.3.5.1 TSS

241 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.

Findings:	The TSS Section 6.10.1 provides a comprehensive description of the Image Overwrite function. The image overwrite security function can also be invoked manually (on demand) by the system administrator (ODIO). A standard On Demand Image Overwrite (ODIO) overwrites all files written to temporary storage areas of the HDD; a full Immediate Image Overwrite (IIO) overwrites those files as well as fax mailbox/dial directory and scan to mailbox data. The description also covers when image data is overwritten.

3.3.5.2 Operational Guidance

242 The evaluator shall check to ensure that the operational guidance contains instructions for enabling the Image Overwrite function.

Findings:	The SIG Section 'Immediate Image Overwrite' describes the settings for configuring Image Overwrite function. On Demand Image Overwrite is explained on pages 17 & 18 of the SIG.

3.3.5.3 Test

243 The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

3.3.6 FDP_RIP.1(b) Subset residual information protection

3.3.6.1 TSS

244 The evaluator shall examine the TSS to ensure that the description is comprehensive in describing what customer-supplied data is to be purged, where it is stored, and how it is made unavailable.

Findings:	The TSS in ST Section 6.10.2 describes the purge function and covers all data to be purged including all jobs that are actively in progress or that are stored on the TOE for later processing; all customer data stored in address books and accounting database. The TOE will reformat the hard drive at the completion of the purge function.

3.3.6.2 Operational Guidance

245 The evaluator shall check to ensure that the operational guidance contains instructions for initiating the Purge Data function.

Findings:	The SIG Section 'Operation of IIO and ODIO' describes the settings for the purge function.

3.3.6.3 Test

246 The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

247

3.4 Identification and Authentication (FIA)

3.4.1 FIA_AFL.1 Authentication Failure Handling

3.4.1.1 TSS

248 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.

Findings:	ST Section 6.1.2 – The TSF will lock user account for 5 minutes after 3 unsuccessful authentication attempts. The description includes the messages displayed by the TSF when a user is locked out at both the EWS and the Control Panel.

3.4.1.2 Operational Guidance

249 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.

Findings:	The SIG Section 'Additional items' describes the settings for authentication failure.

3.4.1.3 Test

250 The evaluator shall also perform the following tests:

251 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.

252 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.

253 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).

254 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.

Findings:	The DTR test case for FIA_AFL.1 configures the authentication failure threshold and creates 3 failed login attempts to show that the account is locked out for the configured 5 minutes. The test demonstrates authentication failure handling at both the LUI and EWS interfaces and shows the messages that the TSF displays at both interfaces.

3.4.2 FIA_ATD.1 User attribute definition

3.4.2.1 TSS

255 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.

Findings:	ST Section 6.3.1 – The TSS describes that the TOE maintains username, password and role security attributes for each individual user. This is consistent with the SFR definition.

3.4.3 FIA_PMG_EXT.1 Extended: Password Management

3.4.3.1 Operational Guidance

256 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.

Findings:	The SIG Section 'Authentication Passwords' provides instructions for password management including password composition and minimum password length.

3.4.3.2 Test

257 The evaluator shall perform the following tests:

258 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.

Findings:	The DTR test case for FIA_PMG_EXT.1 configures the settings for password minimum length and password composition rules, then it creates password of minimum length, less than minimum length and of various combination of characters and verifies that the constraints defined by the SFR are applied.

3.4.4 FIA_UAU.1 Timing of authentication

3.4.4.1 TSS

259 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).

Findings:	ST Section 6.1.1 – the TSS describes local authentication, network authentication (LDAP server), smart card authentication (Windows Domain Controller).

260 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).

Findings:	ST Section 6.1.1 – The TOE performs identification and authentication at the Control Panel and the EWS.

261 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.

Findings:	ST Section 6.8.5– The TOE uses IPsec for communication with the Windows domain controller for Smart Card authentication. ST Section 6.8.3—The TOE uses TLS for communication with LDAP server.

262 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.

Findings:	ST Section 6.1.1 – The TOE will permit jobs request sent via printing protocols before the user is authenticated.

3.4.4.2 Operational Guidance

263 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).

Findings:	The SAG Section 'Authentication' describes the methods of authentication used by the TOE to include local or internal authentication, external authentication with remote LDAP server and Windows Domain controller. The description also covers that the LUI and the WebUI authenticate users with username/password mechanism, and the LUI can also perform smart card authentication.

3.4.4.3 Test

264 The evaluator shall also perform the following tests:

265 1) The evaluator shall check to ensure that identification and authentication succeeds, enabling the access to the TOE when using authorized data.

266 2) The evaluator shall check to ensure that identification and authentication fails, disabling the access to the TOE afterwards when using unauthorized data.

267 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).

Findings:	The evaluator for the DTR testcase for FIA_UAU.1 exercised all methods of user authentication provided by the TOE including internal authentication, external authentication via LDAP, and external authentication via Windows Domain Controller for smart card authentication. The test includes both successful and failed logins with user credentials maintained internally, on the external LDAP server and on the smart card. The evaluator demonstrates that user authentication is successful when using authorized data and unsuccessful when using unauthorized data.

3.4.5 FIA_UAU.7 Protected authentication feedback

3.4.5.1 TSS

268 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.

Findings:	ST Section 6.1.3 – the TSS describes that the TOE obscures the password entered at user login with asterisk characters. This is consistent with the claim made in FIA_UAU.7.

3.4.5.2 Test

269 The evaluator shall also perform the following tests:

270 1. The evaluator shall check to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication.

271 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).

Findings:	The DTR test case for FIA_UAU.7 performs user login at the EWS and the LUI interfaces and verifies that the password entered is obscured with asterisk characters.

3.4.6 FIA_UID.1 Timing of identification

272 It is covered by assurance activities for FIA_UAU.1.

3.4.7 FIA_USB.1 User-subject binding

3.4.7.1 TSS

273 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.

Findings:	The TSS in ST Section 6.3.1 describes the rules for associating security attributes with users. The level of access for the authenticated users is based on their assigned role. This is consistent with the claims made in FIA_USB.1.

3.4.7.2 Test

274 The evaluator shall also perform the following test:

275 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).

Findings:	The DTR test for FIA_USB.1 assigns users different role permissions and verifies that permissions are applied when the user logs in to access TOE functions and protected data.

3.4.8 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

3.4.8.1 TSS

276 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.

Findings:	ST Section 6.8.5 – The TOE supports text-based pre-shared keys of 22 characters. The text-based pre-shared key sequence entered by the user is initially conditioned

	using a SHA-256 hash and then encrypted with AES 256 algorithm. This is consistent with the claims made in FIA_PSK_EXT.1.

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.

Findings:	The ST claims text-based pre-shared keys and no other pre-shared key to use for IPsec.

3.4.8.2 Operational Guidance

277 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.

Findings:	SIG Section ‘IPsec’ – provides guidance on the composition of strong text-based pre-shared keys. The guidance specifies a list of allowable characters that is a super-set of the list contained in the SFR and it provides information on the merits of longer pre-shared keys.

3.4.8.3 Test

278 The evaluator shall also perform the following tests.

279 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.

280 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.

281 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.

282 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.

Findings:	The DTR test case for FIA_PSK_EXT.1 demonstrates 15 successful IPsec negotiations with PSK of 22 characters in all the possible combinations allowed by the SFR. The test also demonstrates IPsec negotiation with PSK of minimum,

	maximum and invalid lengths. Conditional test 3 and test 4 are not applicable as the TOE does not claim support for bit-based pre-shared keys.

3.5 Security management (FMT)

3.5.1 FMT_MOF.1 Management of security functions behavior

3.5.1.1 TSS

283 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.

284 The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.

Findings:	ST Section 6.4.1 references Table 15 for a description of the management functions provided by the TOE. The table outlines the operations that can be performed for each management function and makes clear that only the system administrator can access the listed management functions. The EWS and LUI interfaces are used to manage the TSF and are defined in section 6.1.1 of the ST. This is consistent with the claims made in FMT_MOF.1.

3.5.1.2 Operational Guidance

285 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.

Findings:	The SIG Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ describes the operation methods for the admin to operate the management functions; it covers all management functions described in Table 15 of the ST. “Admin” management functions can be found in section B through E under Part I: Secure Installation and set-up in the evaluated configuration while "normal” user information can be found in section V of Part III: Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration.

3.5.1.3 Test

286 The evaluator shall also perform the following tests:

287 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.

288 2. The evaluator shall check to ensure that the operation results are appropriately reflected.

289 3. The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.

Findings:	The DTR test for FMT_MOF.1 exercises all management functions defined by the SFR as U.ADMIN and demonstrates that U.NORMAL does not see the options to operate the management functions; only the system administrator can see the management options.

3.5.2 FMT_MSA.1 Management of security attributes

3.5.2.1 TSS

290 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.

Findings:	The TSS in ST Section 6.3.2 provides a description of possible operations for security attributes and the roles that can perform these operations. The TSS specifies that unauthenticated users have limited ability while authenticated users and administrators have higher privilege. This is consistent with the claims made for FMT_MSA.1.

3.5.2.2 Operational Guidance

291 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.

292 The evaluator shall check to ensure that the administrator guidance describes the timing of modified security attributes.

Findings:	The SIG Sections ‘Authentication Passwords”, ‘Administrator Password’ and ‘Authorization’ describe the possible operations on security attributes. Except for the login password that can be modified by the owning user, all security attributes are managed by U.ADMIN. The description also covers the timing of modified security attributes.

3.5.2.3 Test

293 The evaluator shall also perform the following tests:

294 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

295 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.

296 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.

Findings:	The evaluator for the DTR test case for FMT_MSA.1 executes all permitted operations on security attributes and demonstrates the management restrictions by showing that the operation completes successfully with admin login and fails with non-admin login. The test shows that the U.NORMAL can manage their own login passwords.

3.5.3 FMT_MSA.3 Static attribute initialization

3.5.3.1 TSS

297 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.

Findings:	ST Section 6.3.2 describes the access configuration for the different types of jobs and the security attributes that have default values. Certain users can access the TOE without authentication and perform print jobs while other types of access require different security attributes such U.NORMAL and U.ADMIN. This is consistent with the claims made for FMT_MSA.3.

3.5.3.2 Test

298 If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP_ACF.1.

3.5.4 FMT_MTD.1 Management of TSF data

3.5.4.1 Operational Guidance

299 The evaluator shall check to ensure that the administrator guidance identifies the management operations and authorized roles consistent with the SFR.

Findings:	SAG section 4 describes the management of TSF data; it covers all TSF data and management operations identified in Table 14 of the ST. Modify login password for authenticated user – SAG section 4 Page 80 “Settings Access Rights” Query authenticated user roles to copy, print, scan or fax on the TOE via the web UI or Local UI – SAG section 4 page 82 “User Permissions” Modify/Change Default authenticated user roles to copy, print, scan or fax on the TOE via the web UI or the local UI – SAG section 4 page 95 “User Permissions” & “User Roles” Modify login password for system administrator – SAG section 4 page 141 “System Administrator Password” Query, or modify the behavior of the audit log – SAG section 4 page 109 “Logs” Modify, query, or delete x.509 certificates (TLS) – SAG section 4 page 123 “Security Certificates” Modify, query or delete IP filter table (rules) – SAG section 4 page 107 “IP Filtering” Modify, query or delete email addresses for fax forwarding – SAG section 4 page 140 “Specifying Email and Internet Fax Recipient Restrictions”

300 The evaluator shall check to ensure that the administrator guidance describes how the assignment of roles is managed.

Findings:	The SIG Section “Authorization” describes how the role assignment is managed.

301 The evaluator shall check to ensure that the administrator guidance describes how security attributes are assigned and managed.

Findings:	The SIG Sections “Authentication” and “Authorization” describe how security attributes are assigned and managed.

302 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.

Findings:	The SIG describes the security-related rules. It covers the access control rules in the 'Authentication' section; timeout is converted in the section 'Session Inactivity Timeout' and user lockout is described in the section 'Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration'.

3.5.4.2 Test

303 The evaluator shall perform the following tests:

304 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.

305 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.

306 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.

Findings:	The DTR test case for FMT_MTD.1 executes all operations permitted on the TSF data and demonstrates the management restrictions by showing that the operation completes successfully with admin login and fails with non-admin login.

3.5.5 FMT_SMF.1 Specification of Management Functions

3.5.5.1 TSS

307 The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.

Findings:	The TSS in ST Section 6.4.1 references Table 16 for the management functions, so the TSS description is consistent with the SFR.

3.5.5.2 Operational Guidance

308 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.

Findings:	The SIG describes the management functions defined by the SFR Table 16. Image Overwrite Security Enable/Disable, Scheduled — SIG Section 'Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration' Enable/Disable and configure Smart Card use — SIG Section 'Configuring Authentication Server Settings for LDAP on the EWS Manage Receive fax (job) passcodes — SIG Section 'Embedded Fax' Configure EWS and LUI session timeout — SIG Section 'Session Inactivity Timeout' Configure users, roles, privileges and passwords — SIG Section 'Authorization'

	Configure network authentication — SIG Section ‘Authentication’ Configure IP filtering — SIG Sections ‘IP Filtering’ and ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ Enable/disable and configure IPsec — SIG Section ‘IPsec’ Enable/disable and configure 802.1x — SIG Section ‘802.1x Device Authentication’ Create/upload/download X.509 certificates — SIG Section ‘Security Certificates’ Enable/disable TLS — SIG Section ‘Transport Layer Security (TLS)’ Transfer the audit records to a remote trusted IT product — SIG Section ‘SFTP Filing’ Configure SFTP — SIG Section ‘SFTP Filing’ Configuration of the audit function — SIG Section ‘Audit Log’ Create a recurrence schedule for Image Overwrite — SIG Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ Invoke Immediate Image Overwrite — SIG Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ Invoke Data Purge Function — SIG Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ Enable/disable and Configure fax forwarding to email — SIG Section ‘Embedded Fax’ Configure Software/Firmware Update — SIG Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’, ‘USB Port Security’ and warning about software/firmware upgrade are in SIG Section ‘Additional Notes’ Configure NTP — SIG Section ‘NTP’ and Section ‘Date and Time’ Configure STARTTLS — SIG Section ‘Scan to Email’

3.5.6 FMT_SMR.1 Security roles

3.5.6.1 TSS

309 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.

Findings:	The TSS in ST Section 6.3.1 describes U.ADMIN and U.NORMAL roles defined by the SFR.

3.5.6.2 Test

310 As for tests of this SFR, it is performed in the tests of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

3.6 Protection of the TSF (FPT)

3.6.1 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

3.6.1.1 KMD

311 The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.

Findings:	KMD Appendix C – keys in non-volatile memory are stored in encrypted file system.

312 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.

Findings:	KMD Appendix C describes the storage location and protection of all keys stored in non-volatile memory.

3.6.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data

3.6.2.1 TSS

313 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.

Findings:	ST Section 6.6.1 — The TSS in Table 17 describes how all cryptographic keys are stored and protected in the TOE. Pre-shared keys, symmetric keys and private keys are protected using encryption.

3.6.3 FPT_STM.1 Reliable time stamps

3.6.3.1 TSS

314 The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.

Findings:	Section 6.2.4 in the ST – The TOE is configured to synchronize with an NTP server to provide reliable time stamps.

3.6.3.2 Operational Guidance

315 The evaluator shall check to ensure that the guidance describes the method of setting the time.

Findings:	The SIG Section ‘NTP’ describes date and time and NTP settings.

3.6.3.3 Test

316 The evaluator shall also perform the following tests:

317 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).

318 2. The evaluator shall check to ensure that the time stamps are appropriately provided.

Findings:	The DTR test for FPT_STM.1 configures NTP, performs an action to generate an audit record, and verifies the time stamp is accurate.

3.6.4 FPT_TST_EXT.1 Extended: TSF testing

3.6.4.1 TSS

319 The evaluator shall examine the TSS to ensure that it details the self-tests that 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.

Findings:	The TSS in ST Section 6.5.1 describes the self-tests ran when the TOE starts to include a trusted boot test, McAfee Embedded Control test, and Cryptographic module verification. The TSS includes an argument that the tests are sufficient to demonstrate correct operation of the TSF.

3.6.4.2 Operational Guidance

320 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.

Findings:	The SIG Section ‘Additional items’ describes the possible errors that may result from the self-tests that are run by the TSF.

3.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

3.6.5.1 TSS

321 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.

Findings:	The TSS in ST Section 6.5.2 describes that the TOE performs signature verification to verify software for update. This is consistent with the SFR.

322 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.

Findings:	The TSS in ST Section 6.5.2 describes that administrator can check the current version of the TOE via both the LUI and EWS. EWS provides the interface to perform updates.

3.6.5.2 Operational Guidance

323 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.

Findings:	The SIG Sections ‘Secure Acceptance’ and Section ‘Secure Operation of Device Services/Functions That Are Part of the Evaluated Configuration’ describe the steps to obtain the TOE version and provide the instructions to start the update process.

3.6.5.3 Test

324 The evaluator shall also perform the following tests:

325 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.

326 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.

327 3. The evaluator shall check to ensure that only administrators can implement the application for updates using authorized data for updates.

328 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.

329 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.)

Findings:	The DTR test for FPT_TUD_EXT.1 shows that the evaluator followed the guidance to check and display the current version of the TOE, performed a successful update of the TOE and verified that the correct TOE version is displayed once the update is complete. The evaluator also changed the signature on the update file, attempted to perform an update, and verified that the signature verification failed causing the update to be unsuccessful. The evaluator also verified that only the administrator can access the update function; non-admin users cannot see the ‘Properties’ options to perform TOE update.

3.7 TOE Access (FTA)

3.7.1 FTA_SSL.3 TSF-initiated termination

3.7.1.1 TSS

330 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.

Findings:	The TSS in ST Section 6.1.2 describes that user session timeout for both the LUI and EWS is configurable by the administrator and includes the default settings.

3.7.1.2 Operational Guidance

331 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.

Findings:	The SIG Section ‘Session Inactivity Timeout’ describes the settings for configuring user session timeout for both the LUI and EWS. The default settings are 60 seconds for the LUI and 60 minutes for EWS.

3.7.1.3 Test

332 The evaluator shall also perform the following tests:

333 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.

334 2. The evaluator shall check to ensure that the session terminates after the specified time interval.

335 3. The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified in the TSS.

Findings:	The DTR test for FTA_SSL.3 describes how the evaluator configured session timeout for both the LUI and EWS, logged in and remained idle past the configured interval of inactivity to demonstrate that the TSF terminates the user session after the configured time interval elapsed.

3.8 Trusted path/channels (FTP)

3.8.1 FTP_ITC.1 Inter-TSF trusted channel

3.8.1.1 TSS

336 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.

Findings:	The TSS in ST Section 6.8 describes the trusted channels communication between the TOE and other authorized IT identities. The TOE uses TLS for communication with LDAP server, SSH for communication with external audit server, and IPsec for communication with a domain controller for smart card authentication. Section 2.2.3 in the ST goes into more detail on how each protocol is used and implemented on the TOE. The SIG describes how to establish communications using TLS, IPsec, and SSH/SFTP. In Section ‘Audit Log Notes’ it also describes recovery when a connection with an authorized IT entity is unintentionally broken.

3.8.1.2 Test

337 The evaluator shall also perform the following tests:

338 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.

339 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.

340 3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.

341 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.

Findings:	The DTR test case for FTP_ITC.1 describes that the evaluator followed the instructions from the SIG to configure IPsec, TLS, and SSH. The evaluator successfully initiated connections to the LDAP server, the audit server and the domain controller, using Wireshark to capture the traffic and to show that the traffic is encrypted. Then the evaluator broke the connection with the external server and used Wireshark to show that once connectivity is restored, the traffic is still protected.

342 Further assurance activities are associated with the specific protocols.

3.8.2 FTP_TRP.1(a) Trusted path (for Administrators)

3.8.2.1 TSS

343 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.

Findings:	ST Section 6.8.1 — The TSS describes that EWS is used for remote administration and access to EWS is protected via TLS/HTTPS. This is consistent with the requirement that TLS/HTTPS be used to protect communication between the TOE and remote administrators.

3.8.2.2 Operational Guidance

344 The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Findings:	The SIG Section ‘Establishing a Remote Session’ describes configuring TLS. EWS is used for remote administration and it is accessed via TLS/HTTPS.

3.8.2.3 Test

345 The evaluator shall also perform the following tests:

346 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.

347 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 session without invoking the trusted path.

348 3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext.

Findings:	The evaluator for the DTR test case for FTP_TRP.1(a) followed the instructions from the SIG to configure TLS. The evaluator successfully logged in to EWS with Wireshark setup to capture the traffic. The evaluator then reviewed the Wireshark capture to verify that the channel data is encrypted. The evaluator also checked that the guidance does not identify interfaces or methods to remotely administer the TOE that do not use TLS/HTTPS.

349 Further assurance activities are associated with the specific protocols.

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

(Modified by NIAP TD 0393)

3.8.3.1 TSS

350 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.

Findings:	ST Section 6.8.1 — The TSS describes that remote non-admin users access the TOE using EWS for scan jobs; EWS communication is protected using TLS/HTTPS. Print client jobs that are sent to the TOE are protected using IPsec.

351 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.

Findings:	The TSS in ST Section 6.8.1 describes that the TOE uses IPsec to secure remote print jobs from print clients and TLS/HTTPS when performing non-admin user access to the EWS, this is consistent with the SFR.

3.8.3.2 Operational Guidance

352 The evaluator shall confirm that the operational guidance contains instructions for establishing the remote user sessions for each supported method.

Findings:	The SIG includes the Section “Establishing a Remote Session” which describes how to establish a remote user session. SIG Section ‘Transport Layer Security (TLS)’ provides instructions for configuring TLS. The TOE uses TLS/HTTPS for access to EWS.

3.8.3.3 Test

353 The evaluator shall also perform the following tests:

354 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.

355 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.

356 3. The evaluator shall ensure, for each method of remote access, the channel data are not sent in plaintext.

Findings:	The DTR Test case for FTP_TRP.1(b) describes that the evaluator configures IPsec and TLS for remote access to the TOE. The evaluator used Wireshark to capture the traffic from the client machine to the TOE, the evaluator sent print jobs and verified that the traffic was encrypted. The evaluator also used Wireshark and logged into the WebUI as the non-admin user and verified that the traffic was encrypted. The evaluator reviewed the SIG and the SAG to confirm that the guidance does not identify an interface for non-admin users to access the TOE without going through the trusted path.

357 Further assurance activities are associated with the specific protocols.

4 Security Assurance Requirements (APE_REQ)

4.1 Class ASE: Security Target evaluation

358 No additional assurance activities

4.2 Class ADV: Development

4.2.1 ADV_FSP.1 Basic functional specification

4.2.1.1 TSS

359 The evaluator shall confirm identifiable external interfaces from guidance documents and examine that TSS description identifies all the interfaces required for realizing SFR.

360 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.

361 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.

362 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.

Findings:	The evaluator reviewed the guidance documentation to catalog the identifiable TSFIs. The TSS identifies the external interfaces that implement the security features of the TOE including the user/administrator interfaces WebUI also called EWS and the LUI, as well as the protocol interfaces to external IT entities including audit log server, LDAP server, Windows domain controller, and print clients via SSH/SFTP, HTTPS, TLS and IPsec. The TSS describes how the TOE implements each SFR. The description of security behavior at the TSFIs is consistent with the SFR claims. The evaluator performed independent testing of the TOE and completed all test assurance activities using the TSS description of the TSFIs as well as the guidance instructions on method of use and configuration parameters needed to realize the SFRs.

4.3 Class AGD: Guidance Documents

4.3.1 AGD_OPE.1 Operational user guidance

4.3.1.1 Operational Guidance

363 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.

364 The evaluator shall check to ensure that the following guidance is provided:

365 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.

Findings:	The SIG in Section V 'Additional items' describes how the administrator can confirm that the TOE returned to its evaluated configuration after a transition from maintenance mode.

4.3.2 AGD_PRE.1 Preparative procedures

4.3.2.1 Operational Guidance

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

Findings:	All MFP platforms claimed in the ST are covered by the guidance provided.

4.4 Class ALC: Life-cycle Support

4.4.1 ALC_CMC.1 Labelling of the TOE

4.4.1.1 Operational Guidance

367 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.

Findings:	Table 1 in the ST identifies the Xerox printer model devices and software version that meet the requirements of the ST. The TOE devices provided for testing are labeled with the model numbers included in the ST and the software version is consistent with the ST. Xerox advertises the Xerox AltaLink printers and the information in the ST is sufficient to distinguish the TOE product from the other Xerox products.

4.4.2 ALC_CMS.1 TOE CM coverage

4.4.2.1 Operational Guidance

368 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.

Findings:	The ST and AGD identify all hardware and software components that comprise the TOE. The evaluator confirmed that for the multi-function printer device models provided for testing, the software version is included in the ST TOE Description. The evaluator also confirmed that the cryptographic modules claimed in the CAVP certificates are included in the TOE.

4.5 Class ATE: Tests

4.5.1 ATE_IND.1 Independent testing - Conformance

4.5.1.1 Test

369 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.

370 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.

371 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.

372 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.

Findings:	The evaluator prepared a detailed test report (DTR) identifying all aspects of the system that was tested and mapping all testing assurance activities to the related tests. The DTR identifies the MFP models used for independent testing and includes an equivalency argument that provides a rationale for selecting the MFP models used for actual testing. The DTR describes the test configurations and tools used for testing. Each SFR test description includes purpose, test steps, expected and actual test results. If a test fails initially and later passes, the actual test results include both the failed and the passed results. The evaluator used the provided guidance to install and configure the TOE for testing. All components of the testing environment are listed in the table below.

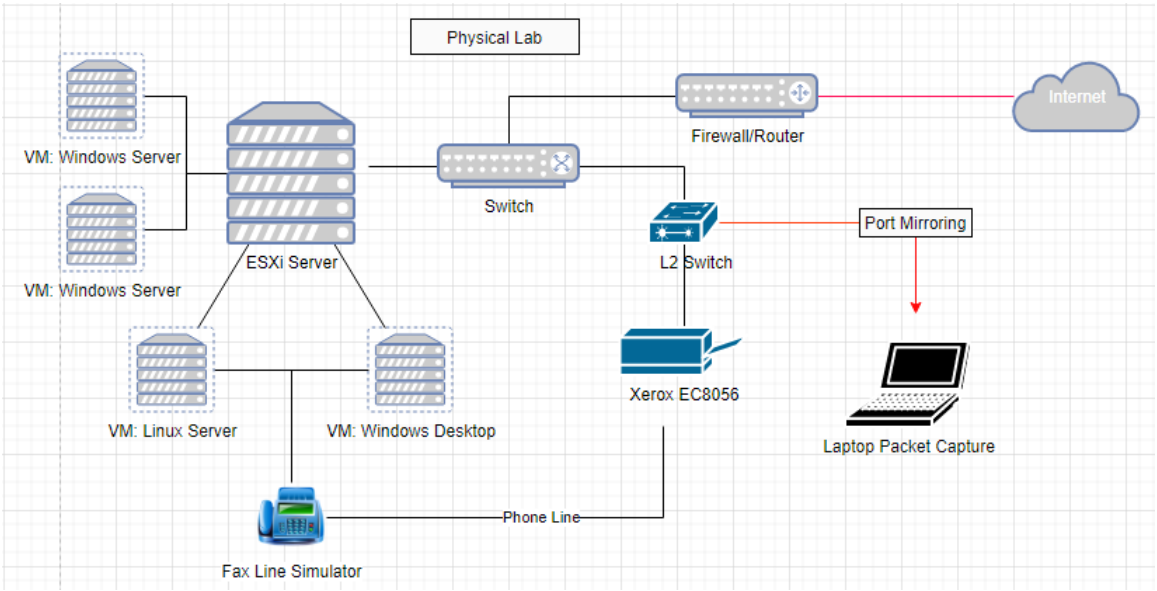

Figure 1 - Test setup

Table 6: Devices Used in the Testing Environment

Device Name	OS Version	Tools
Windows Server 1 (VM)	Windows Server 2019 Standard Edition	Active Directory, Scan to Mailbox Server, Print Server, Window DNS Server, Wireshark.
Windows Server 2 (VM)	Windows Server 2019 Standard Edition	Active Directory, Scan to Mailbox Server, Print Server, Window DNS Server, Wireshark.
Linux Server (VM)	Linux 4.9.0-13-amd64 Debian 4.9.228-1	NTP, Audit Server, FTP Server, TLS Server, TLS Client, IPsec Endpoint, SSH Client, SSH Server, SMTP, Wireshark.
Windows Desktop	Windows 10	TOE Print Drivers, Fax, Wireshark.
ESXi Server	ESXi-6.7.0	N/A
Laptop	Windows 10 Pro	Wireshark

Advanced Phone Line Simulator	Viking Model DLE-300	N/A
Xerox EC8056	103.023.031.35105	N/A

Table 7: Tools Used for Testing

Tool	Version	Tool Location	Tool Purpose
GreenLight	3.0.31	Linux Server (VM)	FCS_TLS_EXT.1 and FCS_SSH_EXT.1 testing
IPSec	strongSwan U5.5.1/K4.9.0-13-amd64	Linux Server (VM)	FCS_IPSEC_EXT.1 testing
Ping	N/A	Linux Server (VM)	FCS_IPSEC_EXT.1 testing
sshd-ls	OpenSSH_7.1p2-Lightship	Linux Server (VM)	FCS_SSH_EXT.1 testing
SNMP	V3	Linux Server (VM)	FAU_STG.4 testing
SMTP	Postfix v3.5.6	Linux Server (VM)	FCS_TLS_EXT.1 testing
LPR	Part of Windows 10	Windows Desktop (VM)	FDP_ACF.1 testing
Xerox Drivers	Version 7.132.19.0	Windows Desktop (VM)	FDP_ACF.1 and FTP_TRP.1(b)
Wireshark	Version 3.2.6	Laptop	Packet captures throughout testing
DNSmasq	Version 2.76	Linux Server (VM)	DNS services
Active Directory	objectVersion 88	Windows Server (VM)	FTP_ITC.1 testing
Cerberus	Version 9.0.5.3	Windows Server (VM)	FCS_SSH_EXT.1 testing
Postfix	Version 3.5.6	Linux Server (VM)	FAU_STG.4 testing
Tera Term	Version 4.105	Laptop	FDP_DSK_EXT.1 and FDP_FXS_EXT.1
OpenSSL	Version 1.0.2g-LS (tls, ssh)	Linux Server (VM)	FCS_TLS_EXT.1 testing
OpenSSH	Version 7.1p2-Lightship	Linux Server (VM)	FCS_SSH_EXT.1 testing

4.6 Class AVA: Vulnerability Assessment

4.6.1 AVA_VAN.1 Vulnerability survey

4.6.1.1 Test

373 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.

374 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.

375 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.

Findings: The DTR includes the vulnerability report. The evaluator performed a search of public information for vulnerabilities that have been reported in printer devices, in the specific TOE printers, and in the communication protocols implemented in the TOE. The evaluator performed searches in accordance with Labgram #116/Valgram #135. The public sources searched included:

- Xerox Security Information, Bulletins and Advisory Responses: https://security.business.xerox.com/
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html
- Wind River CVE Database: https://support2.windriver.com/index.php?page=cve

The evaluator used the following search terms:

- Xerox AltaLink
- Xerox
- Printer
- Multi-Function Printer
- IPsec
- TLSv1.2
- OpenSSL 1.0.2r
- SSH
- SFTP
- Libssh2 v1.7.0
- Wind River Linux
- Mocana

The vulnerability report lists the search results and includes rationale explaining why the TOE is not affected by any of the vulnerabilities returned by the search. The vulnerability search was performed

on April 6th, 2022. Another follow up search was completed on 5/23/2022. The residual vulnerabilities were determined not to be exploitable as the vulnerabilities are only exploitable by a malicious local user or administrator. However, the local users/administrators are assumed to be non-hostile or to be trusted and not to use their privilege for malicious purposes.