ASSURANCE ACTIVITY REPORT

Lexmark Multi-Function Printers with Trusted Platform Module and Hard Drive and without Fax

PREPARED BY
EWA-Canada, An Intertek Company

PREPARED FOR
Communications Security Establishment (CSE) and
National Information Assurance Partnership (NIAP)

REPORT NO
2220-002-D007-2

DOCUMENT VERSION
Version 0.9

DATE
20 June 2023

Contents

The Developer of the TOE:

Lexmark International, Inc.
740 New Circle Road
Lexington 40550
USA

Common Criteria Versions

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017.

Common Evaluation Methodology Versions

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Protection Profiles

- Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015
- Protection Profile for Hardcopy Devices, Version 1.0 Errata #1, June 2017

NIAP Technical Decisions

ITEM	TECHNICAL DECISION TITLE	Comment
TD0157	FCS_IPSEC_EXT.1.1 – Testing SPDs	Updated TSS, guidance, and test assurance activities for FCS_IPSEC_EXT.1.1.
TD0176	FDP_DSK_EXT.1.2 – SED Testing	Updated TSS assurance activity FDP_DSK_EXT.1.2.
TD0219	NIAP Endorsement of Errata for HCD PP v1.0	FCS_COP.1.1(i)
TD0253	Assurance Activities for Key Transport	The TD is associated with FCS_COP.1(i). The TOE does not include FCS_COP.1(i) functionality.
TD0261	Destruction of CSPs in flash	Updated TSS, guidance, and test assurance

ITEM	TECHNICAL DECISION TITLE	Comment
		activities for FCS_CKM.4 Cryptographic Key Destruction
TD0299	Update to FCS_CKM.4 Assurance Activities	Updated test assurance activities for FCS_CKM.4 Cryptographic Key Destruction
TD0393	Require FTP_TRP.1(b) Only for Printing	This is not applicable since the TOE supports printing.
TD0474	Removal of Mandatory Ciphersuite in FCS_TLS_EXT.1	The TD is associated with FCS_TLS_EXT.1. The TOE does not include FCS_TLS_EXT.1 functionality.
TD0494	Removal of Mandatory SSH Ciphersuite for HCD	The TD is associated with FCS_SSH_EXT.1. The TOE does not include FCS_SSH_EXT.1 functionality.
TD0562	Test activity for Public Key Algorithms	The TD is associated with FCS_SSH_EXT.1. The TOE does not include FCS_SSH_EXT.1 functionality.
TD0642	FCS_CKM.1(a) Requirement; P-384 keysize moved to selection	The TOE does not claim elliptic curve digital signature.

Table 1 - NIAP Technical Decisions

1 Introduction

This document presents assurance activity evaluation results of the TOE evaluation. There are three types of assurance activities, and the following is provided for each:

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

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

1.1 Evidence

The following is a list of the documents consulted:

- [ADV_FSP], Lexmark Multi-Function Printers with TPM and Hard Drive and without Fax Functional Specification, 1.12, 2023-02-17
- [AGD_CC-Guide], Common Criteria Installation Supplement and Administrator Guide, December 2022
- [AGD_EWS-Guide], Embedded Web Server Administrator's Guide, 2022-05-31
- [AGD_UserGuide-MachineType7450], Lexmark MX931 MFP User's Guide, 2022-05-01
- [AGD_UserGuide-MachineType7530], Lexmark CX730, CX735, XC4342, XC4352 MFP User's Guide, 2022-02-01
- [AGD_UserGuide-MachineType7580], Lexmark CX930, CX931, XC9325, XC9335 MFP User's Guide, 2022-05-01
- [ALC_CL], Lexmark Multi-Function Printers with TPM and Hard Drive and without Fax Configuration Item List, 1.10, 2023-05-19
- [Crypto_EAR], Lexmark TPM Entropy Assessment Report, 1.6, 2022-12-15
- [Crypto_KMD], Lexmark TPM Key Management Description, 1.4, 2022-11-10
- [ETProcRes], Evaluation Test Plan, Procedures, and Results, 0.8, 2023-06-16
- [HCDPP], Protection Profile for Hard Copy Devices, 1.0, 2015-09-10
- [ETR], Evaluation Technical Report for Common Criteria Evaluation of Lexmark Multi-function Printers with Trusted Platform Module and hard Drive and without Fax and with Firmware Version 081.234, 0.9, 2023-06-20
- [ST], Lexmark Multi-Function Printers with TPM and Hard Drives and without Fax Security Target, 1.13, 2023-05-19

2 Security Functional Requirement Assurance Activities

This section describes the assurance activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The assurance activities are extracted from [HCDPP].

2.1 Security Audit (FAU)

2.1.1 FAU_GEN.1 Audit Data Generation

2.1.1.1 TSS Assurance Activity

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.

Evaluator Assessment:

The auditable events described in the TSS (section 7.1.6) are consistent with the definition of the SFR in section 6.1.1.1. Rather than repeating the events a reference to the auditable events (table 12) in section 6.1.1.1 is provided.

2.1.1.2 Guidance Assurance Activity

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

Evaluator Assessment:

Section "Audit log" in the [AGD_CC-Guide] document specifies the auditable events with their recorded information (date and time of the event is recorded for every auditable event). They are the following:

- Job completed: Recorded information includes JobID, Job_Type, and Job Completed
- Job started: Recorded information includes JobID, Job_Type, and Job ID
- Successful user identification and authentication: Recorded information includes Username and Login successful
- Unsuccessful user authentication: Recorded information includes Login failed with supplied user ID
- Unsuccessful user identification: Recorded information includes Login failed with supplied user ID
- Use of management functions: Recorded information includes Parameter ID and change made including old and new values
- Modification to the group of users that are part of a role: Recorded information includes modification done
- Changes to the time: Recorded information includes confirmation of time change and how
- Failure to establish session: Recorded information includes reason for the failure
- Audit log cleared by an authorized administrator

The auditable events and the recorded information are consistent with the definition of the SFRs.

2.1.1.3 Test Assurance Activity

*The evaluator **shall** also perform the following tests:*

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

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

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

Evaluator Assessment:

The evaluator confirmed that audit records for the following events which are required by the [HCDPP] were generated: job completion (with type of job), unsuccessful user authentication, unsuccessful user identification, use of management functions (i.e. changing security settings or clearing the audit log), modification to the group of users that are part of a role, changes to the time, and failure to establish session (with reason).

The evaluator checked a representative sample for generating auditable events on two interfaces of the Lexmark CX730; the GUI Management TSFI and the Touch Screen TSFI. The evaluator ensured that FIA_UAU.1 events were generated for each of the following mechanisms: Username/Password (local), and LDAP.

It was confirmed that audit events were generated for the GUI and touch screen interfaces.

2.1.2 FAU_GEN.2 User Identity Association

2.1.2.1 Assurance Activity

The Assurance Activities for FAU_GEN.1 address this SFR.

2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

2.1.3.1 TSS Assurance Activity

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

Evaluator Assessment:

Section 7.1.6 of the TSS describes the handling of audit data. Audit records are stored locally and are also sent to a configured external syslog server using IPsec. The records are sent to the syslog server as events are generated. Audit data is stored in the internal log as it is generated.

When the local audit log storage reaches 98% capacity, the oldest records are purged until the used space is lowered to 80% capacity. The local audit log can also be cleared by the administrator in which case an

audit log cleared event will be created.

2.1.3.2 Guidance Assurance Activity

*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.*

Evaluator Assessment:

Section "Setting up Internet Protocol Security (IPSec)" in the [AGD_CC-Guide] document describes how to establish a trusted channel to the audit server. The audit server must be a Syslog server (section Audit log) with the format of the audit logs conforming to RFC5424. The configuration of the TOE needed to communicate with the audit server is discussed in sections "Configuring security audit logging" and "Configuring security audit logging"I in the [AGD_CC-Guide] document].

2.1.3.3 Test Assurance Activity

*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.*

Evaluator Assessment:

For the duration of all testing, the evaluator established an IPsec session between the TOE and the external audit server according to the configuration guidance provided. The evaluator examined traffic that passed between the audit server and the TOE throughout the testing to witness a large amount of audit data being transferred.

The evaluator confirmed using Wireshark that the data was not viewable in the clear during this transfer and confirmed that the data was successfully received by the audit server. For this test, the evaluator configured the SLES 12 SP3 (syslog server with default software rsyslog-8.24.0-12.el7.x86_64) to receive audit records from the TOE. The actual results were consistent with the expected results for this test.

2.2 Cryptographic Support (FCS)

2.2.1 FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric Keys)

TSS Assurance Activity (TD0642)

The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.

Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS.

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

Evaluator Assessment:

Section 7.1.4 of the [ST] describes the use of key establishment for trusted communications. The link

between the claimed cryptographic functionality and the CAVP certificates is provided in section 7.1.10.

2.2.1.1 Test Assurance Activity (TD0642)

The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The 186-4 RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

Evaluator Assessment:

The above test activity was satisfied through the CAVP. The table in section 7.1.10 of the [ST] shows all the CAVP certificates by algorithm and per processor. The SFRs that use the implementation are mapped to the algorithms. The RSA algorithm used has been validated through the CAVP. In the table, there is also a mapping to which SFR the certificate applies. For example, RSA has validation certificates numbers, A2315 and A2309 and is used by FCS_CKM.1(a) and FCS_COP.1(b).

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

2.2.2.1 TSS Assurance Activity

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

Evaluator Assessment:

The functionality described in FCS_RBG_EXT.1 is invoked when the disk encryption functionality is enabled and when the self-signed certificate is generated. FCS_RBG_EXT.1 functionality is also required to generate asymmetric key pairs for IPsec trusted communications. TSS section 7.1.3 describes data encryption and section 7.1.4 describes trusted communications.

2.2.2.2 KMD Assurance Activity

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 used for the encryption/decryption of the user data (FCS_COP.1(d)).

The KMD is described in Appendix F.

Evaluator Assessment:

Lexmark has provided a key management document, [Crypto_KMD], explaining that the TOE relies on the third-party openssl library for random number generation for the disk encryption keys. Section 2.1 of [Crypto_KMD] describes the function call and parameters and the [Crypto_EAR] describes the vendor's assumptions for the amount of entropy seeding the third-party RNG. The key size described in FCS_RBG_EXT is sufficient for the key size and mode used for the encryption/decryption of the user data (FCS_COP.1(d)).

2.2.3 FCS_CKM_EXT.4 Cryptographic Key Material Destruction

2.2.3.1 TSS Assurance Activity

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

Evaluator Assessment:

The disk encryption key is destroyed if the disk encryption functionality is disabled (Table 21 of the [ST]). Session keys are destroyed when the session is terminated (Table 22) of the [ST]. Section 7.1.1 indicates that the TOE maintains passwords used for authentication. These are considered critical security parameters in accordance with the application note for this SFR. The information in [ST] Table 18 indicates that the passwords are destroyed in flash when the account is deleted. Passwords in memory are destroyed at the conclusion of the login.

2.2.3.2 KMD Assurance Activity

The evaluator shall verify the Key Management Description (KMD) includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.

The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4 for the destruction.

Evaluator Assessment:

Section 2 Key Management Description in the [Crypto_KMD] describes where key material resides, how the key material is used, how it is determined that keys are no longer needed, and how the material is destroyed once it is not needed. The keys are used for disk encryption, certificates, PSKs, and IPSec.

Section 2.1 describes the disk encryption key. This key is created when disk encryption is enabled, and it is stored in flash memory so that it is available across reboots. The key is stored in RAM while in use and is destroyed when power is removed from the system.

Section 2.2 describes the certificates, PSKs, and IPSec keys. During TOE installation a self-signed certificate is generated. An administrator may also generate additional certificates or PSKs. These are both stored in flash and are loaded into RAM as required for IPSec communication. IPSec session keys are stored in RAM and these are destroyed when power is removed from the system. When a certificate or PSK is deleted, it is overwritten with zeroes. These keys may exist in flash memory for some period after deletion due to wear levelling and garbage collection.

The description of the key material destruction in the [Crypto_KMD] is consistent with the specification of FCS_CKM.4 in section 6.1.2.4 FCS_CKM.4 Cryptographic key destruction in the [ST] with the cryptographic key destruction being specified to be executed by powering off the device for volatile memory and by the overwriting of the key data storage location with a static pattern for the nonvolatile storage of cryptographic keys.

2.2.4 FCS_CKM.4 Cryptographic Key Destruction

2.2.4.1 TSS Assurance Activity (TD0261)

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

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

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

Evaluator Assessment:

Table 21 - Data Encryption SFR Details in section 7.1.3 Data Encryption in the [ST] states that "Information regarding key destruction is provided in the KMD." Section 6.1.2.4 FCS_CKM.4 Cryptographic key destruction in the [ST] specifies that keys are destroyed by powering off or that zeroes are used to overwrite cryptographic keys. Table 22 – Trusted Communications SFR Details in section 7.1.4 Trusted Communications in the TSS states that destruction of keys in volatile memory is accomplished at power off.

Section 7.1.9 Common Functionality Regarding Key Destruction in Flash Memory states that the storage locations for RSA private keys, PSKs, and the disk encryption key are stored in flash memory and are overwritten with zeroes which is not a value used for any CSPs.

This section also describes how flash wear levelling and garbage collection impact strict conformance to this requirement.

2.2.4.2 KMD Assurance Activity (TD0261)

The evaluator examines the KMD to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory and identifies the memory type (volatile or non-volatile) where key material is stored.

The KMD identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.

Evaluator Assessment:

Section 2 in the [Crypto_KMD] describes where key material resides, how the key material is used, how it is determined that keys are no longer needed, and how the material is destroyed once it is not needed.

Section 2 of [Crypto_KMD] also identifies the different types of keys which are the disk encryption key (DEK) and the certificates, PSKs, and IPSec keys. Section 2.1 describes the DEK and identifies that it is stored in flash memory and temporarily stored in RAM during operation. Section 2.2 describes the certificates, PSKs, and IPSec keys and states that these are stored in flash memory and temporarily stored in RAM during operation.

Section 2.1 of [Crypto_KMD] identifies how the DEK is initialized and used during operation. Section 2.2 describes how an administrator can load PSKs or certificates using the web GUI.

2.2.4.3 Operational Guidance Assurance Activity (TD0261)

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible.

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

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

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. To reduce this risk, the operating system and file system of the OE should support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion. If a RAID array is being used, only set-ups that support TRIM are utilized. If the drive is connected via PCI-Express, the operating system supports TRIM over that channel.

The drive should be healthy and contains minimal corrupted data and should be end of lifed before a significant amount of damage to drive health occurs, this minimizes the risk that small amounts of potentially recoverable data may remain in damaged areas of the drive.

Evaluator Assessment:

[AGD_CC-Guide] includes the section “Erasing keys in flash memory”. This describes the limitations regarding flash memory and the description is consistent with the TSS. The guidance document describes the three types of keys used by the TOE, how they are erased, how wear levelling or garbage collection may allow the keys to temporarily exist in memory, and how the TOE minimizes this risk.

2.2.4.4 Test Assurance Activity (TD0261, TD0299)

For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Cause the TOE to stop the execution but not exit.*
5. *Cause the TOE to dump the entire memory of the TOE into a binary file.*
6. *Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.*

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

Test 2: Applied to each key 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.

1. *Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)*
2. *Cause the TOE to clear the key.*
3. *Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.*

Test 3: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall

use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.*

Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. *Record the storage location of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.*

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

Evaluator Assessment:

The evaluator performed testing at the developer's site which followed the above test steps and confirmed that keys were cleared from memory. A special firmware was loaded on to the TOE which allowed root-access to the underlying hardened Linux OS. The test steps performed by the evaluator are detailed in [ETProcRes] for tests 1 through 4 and were successful. The actual results were consistent with the expected results.

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

2.2.5.1 Test Assurance Activity

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.

Evaluator Assessment:

The above test activity was satisfied through the CAVP. The table in section 7.1.10 of the [ST] shows all the CAVP certificates by algorithm and per processor. The SFRs that use the implementation are mapped to the algorithms. The AES algorithm used in the Lexmark printers have been validated through the CAVP. In the table, there is also a mapping to which SFR the certificate applies. For example, AES (CBC) has validation certificates numbers, A2315, A2309 (88PA6270 (G2)-64bit) and is used by FCS_COP.1(a), FCS_COP.1(d), FCS_IPSEC_EXT.1, and FDP_DSK_EXT.1.

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

2.2.6.1 Test Assurance Activity

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.

Evaluator Assessment:

The above test activity was satisfied through the CAVP. The table in section 7.1.10 of the [ST] shows all the CAVP certificates by algorithm and per processor. The SFRs that use the implementation are mapped to the algorithms. The implemented RSA signature generation and verification was verified as meeting FIPS 186-4 using the 186-4 RSA Validation System (RSA2VS). The TOE generates 2048-bit RSA keys. The RSA implementation was awarded RSA validation certificates A2315 and A2309 and is used by FCS_COP.1(b).

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

2.2.7.1 TSS Assurance Activity

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.

Evaluator Assessment:

Entropy is provided by a hardware based source using CTR_DRBG(AES) and conforms to NIST SP 800-90A. A minimum of 256 bits of entropy is provided by the TRNG. This is described in Sections 7.1.3 and 7.1.4 of the [ST] and is consistent with the selection in FCS_RBG_EXT.1.2.

2.2.7.2 Entropy Description Assurance Activity

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.

Evaluator Assessment:

The [Crypto_EAR] provides all the required information as described in Appendix E including Design Description, Entropy Justification, Operating Conditions, and Health Testing. The evaluator confirms the TOE is providing sufficient entropy when it is generating a Random Bit String.

2.2.7.3 Guidance Assurance Activity

*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.*

Evaluator Assessment:

The administrator does not have to configure the use of the DRBG.

2.2.7.4 Test Assurance Activity

*The evaluator **shall** perform 15 trials for the RBG implementation. If the RBG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator **shall** verify that the instructions in the operational guidance for configuration of the RBG are valid.*

If the RBG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "Generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

*If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator **shall** generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.*

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

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

Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.

Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

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

Evaluator Assessment:

The above test activity was satisfied through the CAVP. The table in section 7.1.10 of the [ST] shows all the CAVP certificates by algorithm and per processor. The SFRs that use the implementation are mapped to the algorithms. The DRBG (AES CTR) achieved CAVP certificates A2315 and A2309 and is used by FCS_RBG_EXT.1.

2.3 User Data Protection (FDP)

2.3.1 FDP_ACC.1 Subset Access Control

2.3.1.1 Assurance Activity

It is covered by assurance activities for FDP_ACF.1.

2.3.2 FDP_ACF.1 Security Attribute Based Access Control

2.3.2.1 TSS Assurance Activity

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

Evaluator Assessment:

Section 7.1.2 of the [ST] describes the functions required to realize the Print and Copy capabilities.

2.3.2.2 Guidance Assurance Activity

The evaluator shall check to ensure to ensure that 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 of the TSS.

Evaluator Assessment:

Each of the user manuals has a section on Printing, Copying, Email, and Scanning. These sections in the user guides, for example, the user manuals for the printers under test [AGD_UserGuide-MachineType7530] and [AGD_UserGuide-MachineType7580], describe the operations related to the parameters to realize the SFP.

2.3.2.3 Test Assurance Activity

The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 2 and Table 3 with each type of interface (e.g., operation panel, Web interfaces) to the TOE.

The evaluator testing should include the following viewpoints:

- representative sets of the operations against 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

Evaluator Assessment:

The various parameters of the SFP were tested and recorded in the test plan, [ETProcRes] "Test Case - Authentication (FIA_UAU.1, FIA_UAU.7, and FIA_UID.1)" tested the copy function and "Test Case - Resource Overwriting (FDP_RIP.1(a)) confirmed that held print jobs weren't available after they had been printed".

2.4 Identification and Authentication (FIA)

2.4.1 FIA_AFL.1 Authentication Failure Handling

2.4.1.1 TSS Assurance Activity

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 attempts, actions to be conducted), which is consistent with the definition of the SFR.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes the actions in case of an administrator configurable number of authentication failures. For logins via the touch panel or web GUI, when the defined number of failed attempts has occurred, the account is locked for an administrator configurable time period.

2.4.1.2 Guidance Assurance Activity

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.

Evaluator Assessment:

Section "Setting login restrictions" in the [AGD_EWS Guide] and section "Configuring login restrictions" in the [AGD_CC-Guide] document discuss the settings for specifying the number of times a user can attempt to log in before being locked out and Lockout time for specifying how long the lockout is to last.

2.4.1.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the subsequent authentication attempts do not succeed by the behavior according to the actions defined in the SFR when unsuccessful authentication attempts reach the status defined in the SFR.

2. The evaluator shall check to ensure that authentication attempts succeed when conditions to re-enable authentication attempts are defined in the SFR and when the conditions are fulfilled.

3. The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication methods when there are multiple Internal Authentication methods (e.g., password authentication, biometric authentication).

4. The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication attempts.

Evaluator Assessment:

The evaluator configured the TOE to lock access to an account for a certain time period after three unsuccessful authentication attempts. The evaluator confirmed that subsequent authentication attempts did not succeed after an account has been locked. The evaluator confirmed that authentication could occur after the account is unlocked after the specified time period. The evaluator performed the tests for both authentication interfaces of the TOE (embedded web server, touch screen). The test steps performed by the evaluator for this test are detailed in [ETProcRes]. The actual results were the same as the expected results.

2.4.2 FIA_ATD.1 User Attribute Definition

2.4.2.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes the security attributes maintained for users. These are listed in the FIA_ATD.1 row in Table 18 and are consistent with those listed in FIA_ATD.1.

2.4.3 FIA_PMG_EXT.1 Password Management

2.4.3.1 Guidance Assurance Activity

*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.*

Evaluator Assessment:

Section “Creating local accounts” in the [AGD_CC-Guide] document provides guidance to security administrators on the composition of passwords (“The password must contain at least one lowercase letter, one uppercase letter, and one nonalphabetic character” and “The password must not contain dictionary words or variations of the user name.”) Section “Configuring the minimum password length” has instructions for setting the minimum password length and recommends that passwords be at least 15 characters. The maximum password length is 32 characters.

2.4.3.2 Test Assurance Activity

*The evaluator **shall** perform the following test:*

*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.*

Evaluator Assessment:

The evaluator has performed testing that used various compositions of valid and invalid passwords. The evaluator confirmed that the TOE supports all ASCII characters, rule characteristics and a minimum length. The evaluator performed edge-case testing on the minimum length to ensure that it is properly enforced by the TOE. The test steps performed by the evaluator for this test are detailed in [ETProcRes].

2.4.4 FIA_UAU.1 Timing of Authentication

2.4.4.1 TSS Assurance Activity

The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).

The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces).

The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers.

The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes the authentication mechanisms provided for the evaluated configuration. These are: smart card authentication, username/password (internal), and username/password (LDAP+GSSAPI). Other than the submission of network print jobs, authentication is required before a user can interact with the TOE. Smart card authentication and LDAP+GSSAPI use Kerberos when authenticating certificates or credentials.

Section 7.1.1 of the [ST] describes the interfaces used for authentication. For smart card authentication, the attached card reader is used for authentication and the touch panel is used to enter a PIN. For the username and password authentication options, the authentication method is the touch panel or the web based administrative interface.

Section 7.1.1 of the [ST] describes the protocols used for authentication. For smart card authentication, the protocol using Kerberos, LDAP and Windows is described. For internal username and password authentication, validation of the password is described. For LDAP+GSSAPI, the protocol is the name of the authentication mechanism, and it is also described in the TSS.

The actions permitted prior to identification and authentication are described in Section 7.1.1 of the [ST]. Specifically, the submission of network print jobs is permitted. Viewing of the operational status of the device is also described.

2.4.4.2 Guidance Assurance Activity

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).

Evaluator Assessment:

A description of LDAP or LDAP+GSSAPI (used for Kerberos) authentication to the TOE is provided in section "Using LDAP or LDAP+GSSAP"I and in section "Creating an LDAP or LDAP+GSSAPI login method" in the [AGD_EWS Guide] document as well as section "Creating a Kerberos login method" in the [AGD_CC-Guide] document. This login method is configured using the web interface. A description of smartcard authentication to the TOE is provided in section "Configuring Smart Card Authentication Client" in the [AGD_CC-Guide] document or in section "Overview" in the [AGD_EWS Guide]. Smartcard authentication is through a smart card reader and the touch screen. A description of local authentication (through the touch screen of the printer or browser session) is provided in section "Using local accounts" in the [AGD_EWS Guide] and in section "Setting up local accounts" in the [AGD_CC-Guide] document.

2.4.4.3 Test Assurance Activity

The evaluator shall also perform the following tests:

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

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

The evaluator shall perform the tests described above for each of the authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces).

Evaluator Assessment:

The evaluator performed tests to ensure that when identification and authentication succeeds, a user is given access to the TOE when using authorized data. The evaluator performed tests to ensure that when identification and authentication fails, a user is unable to access the TOE when using unauthorized data. These tests were repeated for each of the I&A methods (Username/Password, LDAP, Kerberos, and SmartCard) on both interfaces where applicable (embedded web server, touch screen). The test steps performed by the evaluator for this test are detailed in [ETProcRes]. The actual results were the same as the expected results.

2.4.5 FIA_UAU.7 Protected Authentication Feedback

2.4.5.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes the authentication information feedback provided to users while authentication is in progress. For smartcard authentication using the touch panel the TOE displays asterisks and when using the web interface dots are displayed. For username/password accounts the TOE displays

asterisks for both the touch panel and web interface. This is consistent with FIA_UAU.7.

2.4.5.2 Test Assurance Activity

The evaluator shall also perform the following tests:

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

2. The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides (e.g., operation panel, identification and authentication via Web interface).

Evaluator Assessment:

The evaluator performed tests to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication. The evaluator performed this test on both the touch screen and embedded web server. The evaluator confirmed that typed passwords are always displayed as * or ● on either interface. The test steps performed by the evaluator for this test are detailed in [ETProcRes]. The actual results are the same as the expected results.

2.4.6 FIA_UID.1 Timing of Identification

2.4.6.1 Assurance Activity

It is covered by assurance activities for FIA_UAU.1.

2.4.7 FIA_USB.1 User-Subject Binding

2.4.7.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes the rules for associating security attributes with users. New user sessions are initially bound to the default user. This user has no access to functions or data other than being allowed to submit print jobs. User permissions for the session are determined from group memberships. Administrators assign roles to user accounts by configuring permissions for each configured group and then assigning user accounts to groups. For username/password accounts, the permissions for each group that the user is a member of (as specified in the account configuration) are combined. For Smart Cards and LDAP+GSSAPI, a list of group memberships is retrieved from the LDAP server. For each of those groups that match a group configured in the TOE, the permissions are combined. When group memberships or permissions are changed active sessions are not affected. The permissions are described in ST Table 17 - Permissions. This description is consistent with the SFR.

2.4.7.2 Test Assurance Activity

The evaluator shall also perform the following test:

The evaluator shall check to ensure that security attributes defined in the SFR are associated with the users who succeed identification and authentication (it is ensured in the tests of FDP_ACF) for each role that the TOE supports (e.g., User and Administrator).

Evaluator Assessment:

The evaluator performed tests to ensure that the security attributes of Username, Associated Groups, and User permissions were associated with users who succeed identification and authentication for the U.NORMAL and U.ADMIN roles. This included attempting to identify and authenticate, as well as verifying access permissions granted to the groups of which users were a part (and observed that when a user was removed from a group, they no longer had the permissions granted to that group). The test steps performed by the evaluator for this test activity are detailed in [ETProcRes] document. The actual results were consistent with the expected results.

2.5 Security Management (FMT)

2.5.1 FMT_MOF.1 Management of Security Functions Behavior

2.5.1.1 TSS Assurance Activity

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 the definition of the SFR.

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

Evaluator Assessment:

The functions available to administrative users (U.ADMIN) are described in Section 7.1.5 of the [ST]. These functions are consistent with those identified in FMT_MOF.1.

2.5.1.2 Guidance Assurance Activity

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.

Evaluator Assessment:

The “Configuring the printer” section in [AGD_CC-Guide] describes the management functions of the TOE. This includes sections such as “Disabling flash drive access”, and Setting up Internet Protocol Security (IPSec). The [AGD_EWS Guide] also includes details on the use of the management functions (i.e. section “Securing printers”).

2.5.1.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that users of the given roles defined in the SFR can operate the management functions in accordance with the operation methods specified in the administrator guidance.

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

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

Evaluator Assessment:

The evaluator performed tests to ensure that only U.ADMIN had the ability to determine the behaviour of, disable, enable, and modify the behaviour of the functions:

a. Audit;

b. Identification and Authentication;

c. Authorization and access controls;

d. Communication with External IT Entities;

e. Network communications; and

f. System or network time source.

The evaluator confirmed that when operations were performed on the management functions the results of the operations were appropriately reflected. The evaluator performed tests to ensure that U.NORMAL (and any user other than U.ADMIN) did not have access to any of the above operations for the management functions listed. The test steps performed by the evaluator for this test activity are detailed throughout [ETProcRes]. The actual results were consistent with the expected results.

2.5.2 FMT_MSA.1 Management of Security Attributes

2.5.2.1 TSS Assurance Activity

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.

Evaluator Assessment:

Only administrators with the Security Menus permission are able to query, modify, delete or create user accounts or groups. This is stated in Section 7.1.5 of the [ST].

2.5.2.2 Guidance Assurance Activity

The evaluator shall check to ensure that the administrator guidance contains a description of possible operations for security attributes and give roles to those security attributes, which is consistent with the definition of the SFR.

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

Evaluator Assessment:

Section Configuring the printer in the [AGD_CC-Guide] document has a configuration checklist for the timing of modifying security attributes for configuring the printer. The [AGD_EWS Guide] has sections “Managing login methods”, “Managing certificates”, and “Managing other access functions” with information on security operations for security attributes and the roles that apply to those security attributes. This information is consistent with the definition of the SFR.

Where appropriate the administrator guidance includes information on when a change to a security attribute takes effect. For example, in section “Installing a Certificate Authority 9CA) certificate in [AGD_CC-Guide] a reboot of the printer is required when configuring the CA certificate which is used for smart card authentication.

2.5.2.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to the security attributes in accordance with the operation methods specified in the administrator guidance.

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

guidance.

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.

Evaluator Assessment:

The evaluator performed tests to ensure that the TSF restricts to U.ADMIN the ability to query, modify, delete, and create the security attributes of username, associated groups and user permissions.

The evaluator performed tests to ensure that when the security attributes were modified by U.ADMIN, the operation results were appropriately reflected as specified in the administrator guidance. This included but was not limited to: attempting to logon as a deleted user, attempting to access an operation through a user that no longer had the appropriate permission, and deleting a group to which a user belonged and ensuring the user no longer has the permissions associated with that group.

The evaluator ensured that users not part of an authorized role defined in the SFR are not permitted to perform operations on the security attributes. The test steps performed by the evaluator for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

2.5.3 FMT_MSA.3 Static Attribute Initialization

2.5.3.1 TSS Assurance Activity

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.

Evaluator Assessment:

When new users are created, they are associated with no groups and therefore have no permissions. This is described in Section 7.1.5 of the [ST].

2.5.3.2 Test Assurance Activity

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

Evaluator Assessment:

N/A

2.5.4 FMT_MTD.1 Management of TSF Data

2.5.4.1 Guidance Assurance Activity

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

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

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

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

Evaluator Assessment:

Management operations are described in sections “Setting up and using the home screen applications”, “Configuring the e-mail SMTP settings”, and “Secure the printer” in the relevant user guide. The [AGD_EWS Guide] and [AGD_CC-Guide] documents, describe the management functions of the TOE.

The role for a user is dependent on the set of permissions assigned to the user’s account. This is usually done through a group. Section “Setting up local accounts” and “Setting up local groups and permissions” in the [AGD_CC-Guide] and “Using local accounts” in the [AGD_EWS Guide] discuss the editing or deleting of local account groups.

Section Managing login methods in the [AGD_EWS Guide] and section Configuring the printer in the [AGD_CC-Guide] document discuss how security attributes are assigned and managed.

The configuring of the security related rules are described in [AGD_CC-Guide]. For example, “Configuring the minimum password length” and “Configuring login restrictions” describe how to set the minimum password length and the account lockout parameters.

2.5.4.2 Test Assurance Activity

The evaluator shall perform the following tests:

1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to TSF data in accordance with the operation methods specified in the administrator guidance.

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

3. The evaluator shall check to ensure that no users other than users of the given roles defined in the SFR can perform operations to TSF data.

Evaluator Assessment:

The evaluator performed tests to ensure that U.NORMAL and U.ADMIN can perform operations on TSF data in accordance with the operation methods specified in the administrator guidance. Through set up of the test environment and testing of the TOE as documented in [ETProcRes], the evaluator ensured that each operation on TSF Data in Table 13 of [ST] was tested.

For each operation on TSF data, the evaluator ensured that the operation results are appropriately reflected as specified in the administrator guidance.

The evaluator performed tests to ensure that no users other than users of the given roles defined in the SFT can perform operations to TSF data. This included but was not limited to the following: attempting to access data belonging to other users, attempting to access TSF data while unauthenticated to the TOE, configuring permissions, timeouts, and consecutive logon failures.

2.5.5 FMT_SMF.1 Specification of Management Functions

2.5.5.1 TSS Assurance Activity

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

Evaluator Assessment:

The management functions described in Table 24 (in the TSS) are consistent with those described in FMT_SMF.1. Table 24 provides the permissions required by the U.ADMIN user in order to perform the listed functions.

2.5.5.2 Guidance Assurance Activity

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.

Evaluator Assessment:

The management functions for the TOE are described in the user guides (i.e. [AGD_UserGuide-MachineType7530], the [AGD_CC-Guide], and the [AGD_EWS Guide]. The operation of the management functions is described and is consistent with the assignment in the FMT_SMF.1 SFR.

2.5.6 FMT_SMR.1 Security Roles

2.5.6.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.5 of the [ST] describes the security related roles and the description is consistent with FMT_SMR.1.

2.5.6.2 Test Assurance Activity

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

Evaluator Assessment:

N/A

2.6 Protection of the TSF (FPT)

2.6.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data

2.6.1.1 TSS Assurance Activity

*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.*

Evaluator Assessment:

Section 7.1.5 of the [ST] indicates that neither the web interface nor the touch panel provide the ability to view pre-shared keys, symmetric keys or private keys. Section 7.1.4 of the [ST] indicates that session keys (symmetric session keys) are stored in dynamic RAM. Pre-shared keys, symmetric keys and private keys are stored in flash and they cannot be viewed (Table 25, FPT_SKP_EXT.1).

2.6.2 FTP_STM.1.1 Reliable Time Stamps

2.6.2.1 TSS Assurance Activity

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

Evaluator Assessment:

Section 7.1.6 of the [ST] describes the mechanisms for providing reliable time stamps. This is done through the hardware or an NTP service.

2.6.2.2 Guidance Assurance Activity

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

Evaluator Assessment:

Section Setting the date and time in the [AGD_EWS Guide] describes how to configure the date and time maintained by the printer in subsection Configuring manually or maintained by the Network Time Protocol (NTP) in subsection Configuring NTP. Section Configuring time source settings in the [AGD_CC-Guide] document describes how to configure the NTP settings in subsection Configuring NTP settings and how to configure the system clock in the printer in subsection Configuring the system clock manually.

2.6.2.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance or external network services (e.g., NTP).

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

Evaluator Assessment:

The evaluator performed tests to confirm that the time is correctly set up both via manual configuration and via NTP. The evaluator performed tests to ensure that time stamps are appropriately provided and correctly reflect the time. Samples of audit records were generated in order to analyze audit log and syslog data to see if correct timestamps were provided by the TOE. The test steps performed by the evaluator for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

2.6.3 FPT_TST_EXT.1 Extended: TSF Testing

2.6.3.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.7 of the [ST] indicates that self-tests are performed on the cryptographic components. A high level description of the self-tests indicates the functions being tested. A digital signature (RSA 2048, SHA256) of the executable code is calculated and compared to a saved value in flash.

- Memory testing – Fixed values are written to memory and read back to ensure memory is functioning properly.
- Processor testing – Basic arithmetic functions of the processor are verified.
- Cryptographic algorithm testing – Uses Known Answer Tests (KATs) to verify proper operation of cryptographic functions.

The argument that the tests are sufficient to demonstrate that the TSF is operating correctly indicates that the tests verify correct operation of the TOE, and if an error is found, a message indicates the error and suspends operation.

2.6.3.2 Guidance Assurance Activity

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.

Evaluator Assessment:

Section Self-Test in the [ST] document discusses the errors from the self-tests. Since these errors are fatal errors, the administrator would need to contact Lexmark support to resolve them. More details on the self-tests performed are include in section 7.17 Trusted Operation of the [ST].

2.6.4 FPT_TUD_EXT.1 Extended: Trusted Update

2.6.4.1 TSS Assurance Activity

The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

Evaluator Assessment:

Section 7.1.7 of the [ST] describes software update. A digital signature on the new firmware is verified before the update is applied, which is consistent with the SFR. The TSS indicates that the web interface may be used to verify the firmware version and perform updates.

2.6.4.2 Guidance Assurance Activity

*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.*

Evaluator Assessment:

Section Checking physical interfaces and installed firmware in the [AGD_CC-Guide] document discusses how to obtain the firmware version.

Section Updating firmware in the [AGD_CC-Guide] document and in the [AGD_EWS Guide] discusses how to start the firmware update.

2.6.4.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by means of the operation methods specified by the administrator guidance.

2. The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds using authorized data for updates by means of the operation methods specified by the administrator guidance.

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

4. The evaluator shall check to ensure that the updates are correctly performed by obtaining the current version of the TOE after the normal updates finish.

5. The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.)

Evaluator Assessment:

The evaluator confirmed that the current version of the TOE can be queried per the administrator guidance.
The evaluator performed tests to confirm that only an authorized user (U.ADMIN, not U.NORMAL) can perform updates using authorized data.
The evaluator confirmed that when an authorized user updates the TOE using authorized data the TOE is correctly performed.
The evaluator performed tests in which the evaluator uploaded invalid firmware versions and attempted to install them. The evaluator attempted to install the following invalid firmware:
a. A corrupted version of the correct firmware version;
b. A valid firmware version of another printer model; and
c. A valid firmware version with an invalid signature.
The evaluator confirmed that verification of the data for updates of the TOE fails using unauthorized data for updates.
The test steps performed by the evaluator for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

2.7 TOE Access (FTA)

2.7.1 FTA_SSL.3 TSF-Initiated Termination

2.7.1.1 TSS Assurance Activity

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 inactivity.

Evaluator Assessment:

Section 7.1.1 of the [ST] describes termination of user sessions for both the web interface and the touch panel. A smartcard user is terminated when the card is removed. User sessions are also terminated after an administrator configurable period of inactivity range for each interface. The time range for the web interface is from 1 to 120 minutes and for the touch panel is from 10 to 300 seconds.

2.7.1.2 Guidance Assurance Activity

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.

Evaluator Assessment:

Section Configuring login restrictions in the [AGD_CC-Guide] document discusses how to set the Web Login Timeout for remote logins and the Screen Timeout for logging out a user on the home screen. The default value for the Web Login Timeout is 10 minutes and the default value for the Screen Timeout is 60 seconds.

2.7.1.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. If it is settable, the evaluator shall check to ensure that the time until the termination of the session can be set up by the method of setting specified in the administrator guidance.

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

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

Evaluator Assessment:

The evaluator ensured that it is possible to set up the time until session termination occurs can be set up as per administrator guidance.

On each TOE login interface (touch screen, embedded web server), the evaluator authenticated with the TOE and waited for the time interval to be reached. The evaluator performed tests to ensure that sessions terminated on both interfaces after the specified time intervals.

The test steps performed by the evaluator for this test activity are detailed in [ETProcRes].

2.8 Trusted Path/Channels (FTP)

2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

2.8.1.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.4 of the [ST] indicates that IPsec is used to protect communications to authentication servers, remote audit servers, email servers, and network time servers. The IPsec protocol is included in the security claims.

The setting up of IPSec is described in the [AGD_CC-Guide] section ‘Configuring the printer’ / ‘Setting up Internet Protocol Security (IPSec)’. This section describes how to set up the communication between the printer and all network services including authentication, audit, email, and NTP. The IPSec configuration for the connection between the printer and workstation or server is described in [AGD_EWS-Guide] (‘Securing

printers' / 'Securing network connections' / 'Configuring IP Security settings'.

Section Configuring IP Security (IPsec) settings in the [AGD_EWS-Guide] also discusses the configuration of IPSec between the printer and the workstation or server.

2.8.1.2 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE

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

4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Further assurance activities are associated with the specific protocols.

Evaluator Assessment:

Throughout the evaluation, the evaluator examined communications between the TOE and each authorized IT entity to ensure that secure communication is success and no channel data is sent in plaintext. The evaluator performed tests which physically interrupted the TOE's connection with each external IT entity. The evaluator confirmed that when the physical connection is restored, communications are appropriately protected. The test steps performed by the evaluator for this test activity are detailed in [ETProcRes].

2.8.2 FTP_TRP.1(a) Trusted Path (for Administrators)

2.8.2.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.4 of the [ST] describes remote administration. Remote administration is performed via the web interface, which is protected using IPsec. This is consistent with the selections in the requirement, and IPsec is included in the security claims.

2.8.2.2 Guidance Assurance Activity

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

Evaluator Assessment:

Section Setting up Internet Protocol Security (IPSec) in the [AGD_CC-Guide] document discusses the setup

of IPSec communication between the printer and all network services including authentication. Section Configuring IP Security (IPsec) settings in the [AGD_CC-Guide] also discusses the configuration of IPSec between the printer and the workstation or server. Only IPSec is claimed for securing remote administrative sessions.

2.8.2.3 Test Assurance Activity

The evaluator shall perform the following tests:

1. The evaluator shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

2. For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.

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

Further assurance activities are associated with the specific protocols.

Evaluator Assessment:

The evaluator performed tests to ensure that communications using the remote administration method (Lexmark embedded web server) were tested throughout the course of the evaluation.

The evaluator followed operational guidance to ensure that the embedded web server is not accessible by the user to establish a remote administrative session without connecting from an IPsec peer of the printer which has an established Security Association.

The evaluator performed analysis using a packet sniffer (Wireshark) to ensure that the channel data are not sent in plaintext.

The test steps performed by the evaluator for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

2.8.3 FTP_TRP.1(b) Trusted Path (for Non-administrators)

2.8.3.1 TSS Assurance Activity

The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-administrative users are indicated, along with how those communications are protected.

The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are consistent with those specified in the requirement, and are included in the requirements in the ST.

Evaluator Assessment:

As indicated in Section 7.1.4 of the [ST], non-administrators may communicate with the TOE over links protected by IPsec. This is consistent with the requirement, and IPsec is included in the security claims.

2.8.3.2 Guidance Assurance Activity

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

Evaluator Assessment:

Section Setting up Internet Protocol Security (IPSec) in the [AGD_CC-Guide] document discusses the setup of IPSec communication between the printer and all network services including authentication. Section Configuring IP Security (IPsec) settings in the [AGD_EWS Guide] also discusses the configuration of IPSec between the printer and the workstation or server. Only IPSec is claimed for securing remote user sessions.

2.8.3.3 Test Assurance Activity

The evaluator shall perform the following tests:

1. The evaluator shall ensure that communications using each specified (in the operational guidance) remote user access method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

2. For each method of remote 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 user session without invoking the trusted path.

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

Further assurance activities are associated with the specific protocols.

Evaluator Assessment:

The evaluator performed tests to ensure that communications using the remote administration method (Lexmark embedded web server) were tested throughout the course of the evaluation. The evaluator followed operational guidance to ensure that the embedded web server is not accessible by the user to establish a remote user session without connecting from an IPsec peer of the printer which has an established security association.

The evaluator performed tests to ensure that user functionality (i.e., sending a print job) was not available when attempted outside of the trusted path. The evaluator performed analysis using a packet sniffer (Wireshark version) to ensure that the channel data are not sent in plaintext. The test steps performed by the evaluator for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

3 Evaluation Activities for Conditionally Mandatory Requirements

3.1 Confidential Data on Field-Replaceable Nonvolatile Storage Devices

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

3.1.1.1 KMD Assurance Activity

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

The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.

Evaluator Assessment:

Section 2 Key Management Description in the [Crypto_KMD] describes how keys stored in nonvolatile memory are protected.

The keys include the disk encryption key (DEK) and the certificates, PSKs and IPsec keys. Section 2.1 describes the handling of the DEK and states that there is no means to view this key. Section 2.2 describes the certificates, PSKs and IPsec keys. The system loads these from flash into RAM as needed and there is no provision to view or change these values.

3.1.2 FPT_KYC_EXT.1 Extended: Key Chaining

3.1.2.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.3 of [ST] indicates that the key chain supports DEK outputs of no fewer than 256 bits.

3.1.2.2 KMD Assurance Activity

The evaluator shall examine the KMD to ensure that it describes a high level description of the key hierarchy for all accepted BEVs. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap, submask combining, or key encryption.

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

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

Evaluator Assessment:

Section 2 Key Management Description in the [Crypto_KMD] provides a high-level description of the key

hierarchy for all accepted BEVs.

The key chain is described in sufficient detail. Section 2 Key Management Description in the [Crypto_KMD] includes a description of the strength of keys throughout the key chain. The evaluator verified that at no point the chain could be broken without a cryptographic exhaust and the effective strength of the BEV is maintained throughout the Key Chain.

Section 2 Key Management Description in the [Crypto_KMD] how the key chain process does not expose any material that might compromise the keys in the chain.

3.1.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

3.1.3.1 Assurance Activity

In the assurance activities, below, "Device" refers to the Field-Replaceable Nonvolatile Storage Device from FDP_DSK_EXT.1. If the TOE contains more than one applicable Device, then the assurance activities are performed as necessary on each such Device.

3.1.3.2 TSS Assurance Activity (TD0176)

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.

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied.

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.

Evaluator Assessment:

The self-decrypting device option has not been selected in FDP_DSK_EXT.1.1.

Data encryption is described in Section 7.1.3 of the [ST]. This section describes the types of data written to the disk, how the data is encrypted and when the data is encrypted. It is encrypted as it is written to the disk.

All of the cryptographic functions are provided by the TOE.

Disk encryption is only enabled when the TOE is put into the evaluated configuration (initially provisioned). Disk encryption implements encryption of the entire disk.

3.1.3.3 Guidance Assurance Activity

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.

Evaluator Assessment:

Hard disk encryption is automatic when a hard drive is installed and does not require any user intervention.

3.1.3.4 KMD Assurance Activity

The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the Device's interface and the Device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine. The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area). The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. If encryption can be enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of confidential data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Evaluator Assessment:

Section 2. Key Management Description in the [Crypto_KMD] contains the following information:
- A description of the data encryption engine, its components, and details about its implementation;
- A functional (block) diagram showing the activities the TOE performs to ensure it encrypts the storage device entirely when an administrator first provisions the product;
- Instructions to ensure that when encryption is enabled, the TOE encrypts the Field-Replaceable Nonvolatile Storage Device;
- The data flow from the interface to the Field-Replaceable Nonvolatile Storage Device's persistent media storing the data;
- Conditions in which the data bypasses the data encryption engine; and
- A description of the system and the encryption initialization.

3.1.3.5 Test Activity

The evaluator shall perform the following tests:

Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of Use documents and Confidential TSF data.

Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material.

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

Evaluator Assessment:

The evaluator performed testing at the developer's site to ensure that data written to the hard disk drive is encrypted. Known data was sent to the TOE which was subsequently stored in memory (i.e., held print jobs). The evaluator then removed the hard disk from the TOE and analyzed it to ensure that none of the known data was present in plaintext. The evaluator then confirmed that the data could be decrypted and

made available.

The test steps performed for this test activity are detailed in [ETProcRes]. The actual results were consistent with the expected results.

4 Evaluation Activities for Optional Requirements

4.1 Internal Audit Log Storage

4.1.1 FAU_SAR.1 Audit Review

4.1.1.1 TSS Assurance Activity

The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by authorized users and functions to view audit records.

The evaluator shall check to ensure that the TSS contains a description of the methods of using interfaces that retrieve audit records (e.g., methods for user identification and authentication, authorization, and retrieving audit records).

Evaluator Assessment:

Section 7.1.6 of the [ST] indicates that Administrators with the Security Menu permission may view audit records using the web interface. Section 7.1.1 of the [ST] describes identification and authentication required to access the web interface.

4.1.1.2 Guidance Assurance Activity

*The evaluator **shall** check to ensure that the operational guidance appropriately describes the ways of viewing audit records and forms of viewing.*

Evaluator Assessment:

Section “Configuring security audit log settings” in the [AGD_EWS Guide] states that security logs are stored on the device and may also be transmitted to a syslog server. Section Audit log in the [AGD_CC-Guide] document mentions that the security log can also be exported through e-mail or viewed through the web GUI.

4.1.1.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the forms of audit records are provided as specified in the operational guidance by retrieving audit records in accordance with the operational guidance.

2. The evaluator shall check to ensure that no users other than authorized users can retrieve audit records.

3. The evaluator shall check to ensure that all audit records are retrieved by the operation of the retrieving audit records.

Evaluator Assessment:

The evaluator confirmed that the audit record is provided as specified in the operational guidance by retrieving the audit records via the Lexmark embedded web server in accordance with the operational guidance.

The evaluator confirmed that no other users other than an authorized user/administrator (U.ADMIN) can retrieve the audit records.

The evaluator confirmed that all audit records are retrieved by the operation of retrieving audit records.

The test steps that the evaluator performed to execute the above tests are described in [ETProcRes]. The

actual results were consistent with the expected results

4.1.2 FAU_SAR.2 Restricted Audit Review

4.1.2.1 Test Assurance Activity

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

Evaluator Assessment:

The evaluator confirmed that audit records could not be read prior to authentication and that they could not be read by unauthorized users ([ETProcRes] Test Case - Restricted Audit Review (FAU_SAR.2 and FAU_STG.1)).

4.1.3 FAU_STG.1 Protected Audit Trail Storage

4.1.3.1 TSS Assurance Activity

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

Evaluator Assessment:

Section 7.1.6 of the [ST] indicates that only Administrators with the Security Menu permission may clear the internal audit log. There is no interface that provides a means of modifying audit records.

4.1.3.2 Guidance Assurance Activity

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

Evaluator Assessment:

Section 7.1.6 of the [ST] states that audit records are stored internally and sent to a configured remote syslog server. The syslog protocol is used to provide the audit records to the remote syslog server and IPsec is used for communication. Only administrators with the Security Menu permission may upload the audit log in syslog or CSV format using their browser. Clearing of the audit log is also restricted to administrators. There is no mechanism to modify audit records.

Section “Configuring the printer” of [AGD_CC-Guide] contains a configuration checklist and details the setup of IPSec, audit log, login restrictions, groups, and permissions, In the [AGD_EWS Guide] section “Configuring security audit log settings” describes how an administrator configures the audit log settings and how the log can be exported.

The TSS and operational guidance are consistent.

4.1.3.3 Test Assurance Activity

The evaluator shall also perform the following tests:

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

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

Evaluator Assessment:

The evaluator performed tests to ensure that only authorized users (U.ADMIN) can access the audit records.

The evaluator also confirmed that a user (U.NORMAL) who is unauthorized to access the audit records is unable to access the audit records.

The test steps that the evaluator performed to execute this test are described in [ETProcRes]. The actual results were consistent with the expected results.

4.1.4 FAU_STG.4 Prevention of Audit Data Loss

4.1.4.1 TSS Assurance Activity

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.

Evaluator Assessment:

When the audit logs reach 98% capacity, the oldest logs are removed until the storage space reaches 80% capacity. This is described in Section 7.1.6 of the [ST] and is consistent with FAU_STG.4.

4.1.4.2 Guidance Assurance Activity

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.

Evaluator Assessment:

Section “Configuring security audit logging” in the [AGD_CC-Guide] document and section “Configuring security audit log settings” in the [AGD_EWS Guide] specifies that the oldest log entries are overwritten when the log becomes full. The TOE can send an e-mail message to administrators informing them when the log becomes full and begins to overwrite the oldest entries.

4.1.4.3 Test Assurance Activity

The evaluator shall also perform the following tests:

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

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

Evaluator Assessment:

The evaluator performed testing which caused auditable events to be generated after the capacity of audit records on the printer became full. The evaluator verified that an e-mail alert is sent after the audit log reaches the set percentage of its capacity and that audit events were generated.

The evaluator confirmed that the oldest records were overwritten when the audit log reached near-full capacity as specified in FAU_STG.4

The test steps that the evaluator performed to execute this test are described in [ETProcRes]. The actual results were consistent with the expected results.

4.2 Image Overwrite

4.2.1 FDP_RIP.1(a) Subset Residual Information Protection

4.2.1.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.8 of the [ST] describes data clearing and purging. It includes an account of where the data is stored and how and when it is overwritten.

4.2.1.2 Guidance Assurance Activity

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

Evaluator Assessment:

The TOE automatically overwrites completed jobs. No instructions are needed for enabling this functionality.

4.2.1.3 Test Assurance Activity

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

Evaluator Assessment:

The evaluator performed testing at the developer's site which caused the TOE to overwrite known data. The evaluator examined TOE memory to confirm that the overwrite function had executed successfully. The test steps performed by the evaluator for this test are detailed in [ETProcRes]. The actual results were the same as the expected results.

4.3 Purge Data

4.3.1 FDP_RIP.1(b) Subset Residual Information Protection

4.3.1.1 TSS Assurance Activity

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.

Evaluator Assessment:

Section 7.1.8 of the [ST] describes data clearing and purging. The subject of purging is the job data, which is described in detail in Section 7.1.2. The data is stored on the disk that is subject to the purge operation. A description of the purge function describes how the data is made unavailable.

4.3.1.2 Guidance Assurance Activity

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

Evaluator Assessment:

Sections "**Erasing printer memory"** and "**Erasing printer storage memory"** in the [AGD_EWS Guide] have instructions for erasing printer nonvolatile memory and erasing the hard disk, respectively. Sections "Erasing printer memory' and "erasing printer storage drive" in the user guides (i.e. [AGD_UserGuide-MachineType7530]) also have instructions for erasing printer nonvolatile memory and erasing the hard disk.

4.3.1.3 Test Assurance Activity

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

Evaluator Assessment:

The evaluator included Test Case - Resource Not Available (FDP_RIP.1(b) in the [ETProcRes] document which describes the test related to this function. This test case demonstrates that customer provided information is protected.

5 Evaluation Activities for Selection-Based Requirements

5.1 Confidential Data on Field-Replaceable Nonvolatile Storage Devices

5.1.1 FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)

5.1.1.1 TSS Assurance Activity

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

Evaluator Assessment:

AES for disk encryption uses 256-bit keys and CBC-mode. This is described in Section 7.1.3 of the [ST].

5.1.1.2 Guidance Assurance Activity

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.

Evaluator Assessment:

Encryption is performed using AES and CBC mode. There are no options for other algorithms or modes.

5.1.1.3 Test Assurance Activity

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

AES-CBC Tests

AES-CBC Known Answer Tests

There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.

KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AESCBC decryption.

KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].

To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext

pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost I bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CBC Monte Carlo Tests

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:

```
# Input: PT, IV, Key
for i = 1 to 1000:
    if i == 1:
        CT[1] = AES-CBC-Encrypt(Key, IV, PT)
        PT = IV
    else:
        CT[i] = AES-CBC-Encrypt(Key, PT)
        PT = CT[i-1]
```

The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AESCBC-Decrypt.

AES-GCM Test

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

128 bit and 256 bit keys

***Two plaintext lengths**. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.*

***Three AAD lengths**. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.*

***Two IV lengths**. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested. The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the*

ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

XTS-AES Test

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

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

***Three data unit (i.e., plaintext) lengths**. One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller.*

The evaluator shall test the encrypt functionality using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTSAES encrypt with XTS-AES decrypt.

Evaluator Assessment:

The algorithms used in the TOE were tested by the CAVP. Section 7.1.10 of the [ST] has a table showing which certificate number was issued for AES: A2315/A2309 (88PA6270 (G2)-64bit).

5.2 Protected Communications

5.2.1 FCS_IPSEC_EXT.1 Extended: IPsec (TD0157)

5.2.1.1 TSS Assurance Activity

FCS_IPSEC_EXT.1.1 (TD0157)

The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

FCS_IPSEC_EXT.1.2

The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).

FCS_IPSEC_EXT.1.3

The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no "rules" are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

FCS_IPSEC_EXT.1.4

The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).

FCS_IPSEC_EXT.1.5

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

FCS_IPSEC_EXT.1.6

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKVEv2 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.

FCS_IPSEC_EXT.1.7

The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.

FCS_IPSEC_EXT.1.8

None defined.

FCS_IPSEC_EXT.1.9

The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

FCS_IPSEC_EXT.1.10

The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.

Evaluator Assessment:

FCS_IPSEC_EXT.1.1

Section 7.1.4 Trusted Communications in the [ST] discusses the implementation of the SPD and the processing of inbound and outbound packets. The datagrams that do not use IPSec with ESP (Encapsulating Security Payload) are discarded. The SPD is dynamically built and has accept/protect rules for each IP address with which the TOE communicates and there is a configured pre-shared key or certificate. The SPD has a default 'final rule' to discard all other traffic so that any IP datagram not from a configured IPSec association is discarded.

FCS_IPSEC_EXT.1.2

Both FCS_IPSEC_EXT.1.2 and Section 7.1.4 of the [ST] indicate that transport mode is supported.

FCS_IPSEC_EXT.1.3

Section 7.1.4 of the [ST] indicates that packets are processed against the SP and describes the rules that are implemented. Incoming packets from authorized addresses are accepted and all other IP datagrams are discarded. The SPD has a default 'final rule' to discard packets not from any authorized address.

FCS_IPSEC_EXT.1.4

The ESP cryptographic algorithms are described in Section 7.1.4 of the [ST]. The SHA-based HMAC algorithms listed are included in FCS_COP.1(g).

FCS_IPSEC_EXT.1.5

Section 7.1.4 of the [ST] indicates that both IKEv1 and IKEv2 are supported.

FCS_IPSEC_EXT.1.6

Section 7.1.4 indicates that AES-CBC-128 and AES-CBC-256 are used for encryption, and that IKEv1 and IKEv2 are supported.

FCS_IPSEC_EXT.1.7

Section 7.1.4 of the [ST] indicates that Main Mode is always used for IKEv1 exchanges, and that aggressive mode is never used.

FCS_IPSEC_EXT.1.9

This SFR states that only DH group 14 is supported. Section 7.1.4 of the [ST] indicates that group 14 may be used and indicates how the DH group is negotiated with the peer.

FCS_IPSEC_EXT.1.10

Section 7.1.4 of the [ST] contains a description of the IKE peer authentication process. This description specifies use of the RSA signature algorithm and pre-shared keys as specified in the requirement.

5.2.1.2 Guidance Assurance Activity

FCS_IPSEC_EXT.1.1 (TD0157)

The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

FCS_IPSEC_EXT.1.2

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

FCS_IPSEC_EXT.1.3

The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.

FCS_IPSEC_EXT.1.4

The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the algorithms selected by the ST author.

FCS_IPSEC_EXT.1.5

The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test if IKEv2 is selected.

FCS_IPSEC_EXT.1.6

The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.

FCS_IPSEC_EXT.1.7

If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.

FCS_IPSEC_EXT.1.8

The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that the values allow for Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently, there are no values mandated for the number of packets or number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

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."

FCS_IPSEC_EXT.1.9

None defined.

FCS_IPSEC_EXT.1.10

None defined.

Evaluator Assessment:

FCS_IPSEC_EXT.1.1 (TD0157)

"Setting up Internet Protocol Security (IPSec)" of [AGD_CC-Guide] describes how to configure IPSec. By default, all non IPSec or GUI management port traffic is discarded and this is not configurable.

FCS_IPSEC_EXT.1.2

The TOE only supports transport mode.

FCS_IPSEC_EXT.1.3

By default, all non IPSec or GUI management port traffic is discarded and this is not configurable.

FCS_IPSEC_EXT.1.4

The TOE only supports the setting of the PSK.

FCS_IPSEC_EXT.1.5

The TOE only supports the setting of the PSK and does not support NAT traversal.

FCS_IPSEC_EXT.1.6

The TOE only supports the setting of the PSK.

FCS_IPSEC_EXT.1.7

The TOE only supports the setting of the PSK.

FCS_IPSEC_EXT.1.8

The setting of the SA lifetimes is described in "Setting up Internet Protocol Security (IPSec)" of [AGD_CC-Guide]. The evaluator confirmed during testing that SA lifetimes can be configured, and the claimed time limits are supported. The PP guidance regarding the lifetimes and rekeying timing considerations at each endpoint was applied during testing.

5.2.1.3 Test Assurance Activity

FCS_IPSEC_EXT.1.1 (TD0157)

The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.

FCS_IPSEC_EXT.1.2

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

1. (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.

2. (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.

FCS_IPSEC_EXT.1.3

The evaluator shall perform the following test:

The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that it was not permitted to flow to any of the TOE's interfaces.

FCS_IPSEC_EXT.1.4

The evaluator shall also perform the following tests:

The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the selected algorithms, and attempt to establish a connection using ESP. The connection should be successfully established for each algorithm.

FCS_IPSEC_EXT.1.5

(conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal 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.

NOTE: As per the Errata, it is possible to select IKEv2 as well as "no NAT traversal" so this test would not be applicable.

FCS_IPSEC_EXT.1.6

The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.

FCS_IPSEC_EXT.1.7

The evaluator shall also perform the following test:

(conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.

FCS_IPSEC_EXT.1.8

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

1. (Conditional): The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated.

2. (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

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

FCS_IPSEC_EXT.1.9

The evaluator shall also perform the following test (this may be combined with other tests for this component, for instance, the tests associated with FCS_IPSEC_EXT.1.1):

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

FCS_IPSEC_EXT.1.10

The evaluator shall also perform the following test:

For each supported signature algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection.

Evaluator Assessment:

FCS_IPSEC_EXT.1.1

The evaluator performed tests to ensure that the rules for PROTECT and DROP are properly enforced. Different scenarios were constructed to verify the authenticity of the rules. These scenarios were positive and negative tests such as the following:

a. Two packets matched against a subnet rule; one lacking the IPsec device certificate and the other possessing it);

b. A PROTECT rule established for an external IT entity, but the IT entity lacks the pre-shared key necessary for communicating via IPsec; and

c. Overlapping rules where the subnet of an external IT entity is listed, and the specific IP itself. The first uses a certificate as a method of authentication while the second uses an incorrect IPsec key. Using a network sniffer to capture packets, the evaluator verified that the TOE exhibited the appropriate behaviour for each scenario. Packets matching the DROP rule were not acknowledged and packets matching the PROTECT rule were appropriately encapsulated by IPsec. The test steps performed by the evaluator for this test are detailed in Test Case – IPSec Algorithm FCS_IPSEC_EXT.1.1 and FCS_IPSEC_EXT.1.10 of the [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.2

The evaluator used the operational guidance to configure the TOE to operate in transport mode and also configured an IPsec Peer to operate in transport mode. The evaluator configured the TOE and the IPsec Peer to use the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiated a connection from the TOE to connect to the IPsec Peer. The evaluator observed (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode. The test steps performed by the evaluator for this test are detailed in Test Case – Transport Mode FTP_ITC.1 and FCS_IPSEC_EXT.1.2 of the [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.3

Section 7.1.4 of the [ST] indicates that packets are processed against the SP and describes the rules that are implemented. Incoming packets from authorized addresses are accepted and all other IP datagrams are discarded. Test Case – Discarding Packets FCS_IPSEC_EXT.1.3 was done in conjunction with the tests performed by the evaluator in Test Case – IPSec Algorithm FCS_IPSEC_EXT.1.1 and FCS_IPSEC_EXT.1 of the ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.4

The evaluator configured 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 was successfully established for each algorithm. The test steps performed by the evaluator for this test are

detailed in Test Case – IPSec Protocols FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6, and FCS_IPSEC_EXT.1.9 of the [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.5
Test Case – IPSec Main Mode FCS_IPSEC_EXT.1.7 and Test Case – IPSec SA Lifetime FCS_IPSEC_EXT.1.8 of [ETProcRes] showed that both IKEv1 and IKEv2 are supported. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.6
The evaluator configured 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 confirmed the algorithm was that used in the negotiation. The test steps performed by the evaluator for this test are detailed in Test Case – IPSec Protocols FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6, and FCS_IPSEC_EXT.1.9 of the [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.7

The evaluator configured the TOE as indicated in the operational guidance, and attempted to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt failed. The evaluator then showed that main mode exchanges are supported. The test steps performed by the evaluator for this test are detailed in Test Case – IPSec Main Mode FCS_IPSEC_EXT.1.7 of [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.8

Each of the following tests was performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:
The evaluator constructed 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 observed that this SA is closed or renegotiated in 24 hours or less.

Additionally, the evaluator performed a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.

The test steps performed by the evaluator for each test are detailed in Test Case – IPSec SA Lifetime FCS_IPSEC_EXT.1.8 of [ETProcRes]. The actual results were consistent with the expected results.

FCS_IPSEC_EXT.1.9
This test was combined with other tests for this component. For instance, the tests associated with FCS_IPSEC_EXT.1.1 (Test Case – IPSec Algorithm FCS_IPSEC_EXT.1.1 and FCS_IPSEC_EXT.1.10 and Test Case – IPSec Protocols FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6, and FCS_IPSEC_EXT.1.9 of [ETProcRes]. The actual results were consistent with the expected results).

FCS_IPSET_EXT.1.10

For each supported signature algorithm, the evaluator tested that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection. The test is described in Test Case – IPSec Algorithm FCS_IPSEC_EXT.1.1 and FCS_IPSEC_EXT.1.10 of [ETProRes].

5.2.2 FCS_COP.1(g) Cryptographic Operation (for Keyed-hash Message Authentication)

5.2.2.1 Test Assurance Activity

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.

Evaluator Assessment:

HMAC was tested and validated by the CAVP. Section 7.1.10 has a table that identifies the CAVP certificates which are A2315 and A2309 for HMAC.

5.2.3 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

5.2.3.1 TSS Assurance Activity

The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning.

If "bit-based pre-shared keys" is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based preshared 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.

Evaluator Assessment:

Section 7.1.4 of the [ST] describes the use of pre-shared keys. Pre-shared keys may be 1 to 256 characters in length and are conditioned using SHA-1 or SHA-256. The conditioning is consistent with the selection in the requirement.

Bit-based pre-shared keys was not selected in the SFR.

5.2.3.2 Guidance Assurance Activity

*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.*

Evaluator Assessment:

The passwords are configurable and what is given are the password rules for the evaluated configuration which are only in the ST and the PP. This can be entered in the settings>security>login – add user page. Password information can be found in [AGD_EWS_Guide] and the [AGD_CC-Guide].

5.2.3.3 Test Assurance Activity

The evaluator shall also perform the following tests:

1. The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed characters in various combinations that conform to the operational guidance and demonstrates that a successful protocol negotiation can be performed with each key.

2. [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.

3. [conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key

4. [conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

Evaluator Assessment:

The evaluator performed testing with the following pre-shared key compositions:

a. 15 pre-shared keys of 22 characters which were composed of randomly selected characters from the list of supported characters;

b. 15 pre-shared keys of 1 character (minimum length) which were composed of randomly selected characters from the list of supported characters;

c. 15 pre-shared keys of 36 characters (maximum length) which were composed of randomly selected characters from the list of supported characters; and

d. 15 pre-shared keys of 258 characters (invalid length) which were composed of randomly selected characters from the list of supported characters.

The evaluator confirmed that the TOE was successfully able to establish a connection with an IPsec Peer using the valid pre-shared keys from point a to point c. The evaluator confirmed that the TOE was unable to establish a connection with an IPsec Peer using the invalid pre-shared keys from point d. The test steps performed by the evaluator for this test are detailed in [ETProcRes]. The actual results were the same as the expected results.

5.3 Trusted Update

5.3.1 FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)

5.3.1.1 TSS Assurance Activity

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.

Evaluator Assessment:

The association of hash functions with other TSF cryptographic functions is documented in the TSS. Section 7.1.4 describes the cryptographic functions used for trusted communications and section 7.1.7 describes the cryptographic functions used to verify the executable's digital signature.

5.3.1.2 Guidance Assurance Activity

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.

Evaluator Assessment:

In IPSec Secure Mode of operation (TOE) hashing sizes are not configurable in the Lexmark printers. These functions are restricted to predefined selections, as a result configuration of hashing sizes are not present in the guidance documentation for the Lexmark printer models.

Test Assurance Activity:

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

*The evaluator **shall** perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.*

Short Messages Test - Bit-oriented Mode

*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.*

Short Messages Test - Byte-oriented Mode

*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.*

Selected Long Messages Test - Bit-oriented Mode

*The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text **shall** be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.*

Selected Long Messages Test – Byte-oriented Mode

*The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text **shall** be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.*

Pseudorandomly Generated Messages Test

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.

Evaluator Assessment:

The algorithms used in the TOE were tested by CAVP. Section 7.1.10 of the [ST] has a table indicating that SHA algorithm received CAVP certificates A2315/A2309 (88PA6270 (G2)-64bit).

6 Security Assurance Requirement Activities

The sections below specify EAs for the Security Assurance Requirements (SARs) included in the related cPPs (see section 1.1 above). The EAs in Section 2 (Evaluation Activities for SFRs), Section 3 (Evaluation Activities for Optional Requirements), and Section 4 (Evaluation Activities for Selection-Based Requirements) are an interpretation of the more general CEM assurance requirements as they apply to the specific technology area of the TOE.

In this section, each SAR that is contained in the cPP is listed, and the EAs that are not associated with an SFR are captured here, or a reference is made to the CEM, and the evaluator is expected to perform the CEM work units.

6.1 ASE: Security Target Evaluation

6.1.1 General ASE

When evaluating a Security Target, the evaluator performs the work units as presented in the CEM. In addition, there may be Assurance Activities specified within the PP that call necessary descriptions to be included in the TSS that are specific to the TOE technology type.

Appendix E provides a description of the information expected to be provided regarding the quality of entropy in the random bit generator.

Evaluator Assessment:

The evaluator evaluated the [ST] using the work units in the CEM. The appropriate SFRs in the PP are in the [ST].

Given the criticality of the key management scheme, this PP requires the developer to provide a detailed description of their key management implementation. This information can be submitted as an appendix to the ST and marked proprietary, as this level of detailed information is not expected to be made publicly available. See Appendix F for details on the expectation of the developer's Key Management Description.

Evaluator Assessment:

The vendor has provided a key management document [Crypto_KMD] which is submitted with this AAR.

6.2 ADV: Development

For TOEs conforming to this PP, the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 4, Appendix B, Appendix C, and Appendix D should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

Evaluator Assessment:

The vendor has supplied a functional specification [ADV_FSP] along with the [Crypto_KMD] and the [Crypto_EAR]. The [ADV_FSP] and the TSS are consistent.

6.2.1 ADV_FSP.1 Basic Functional Specification

The functional specification describes the TSF Interfaces (TSFIs). At the level of assurance provided by this PP, it is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users (to include administrative users), at this assurance level there is little point specifying that such interfaces be described in and of themselves since only indirect

testing of such interfaces may be possible. The activities for this family for this PP should focus on understanding the interfaces presented in the TSS in response to the functional requirements, and the interfaces presented in the AGD documentation. No additional "functional specification" document should be necessary to satisfy the assurance activities specified. The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

CEM ADV_FSP.1 Work Units	Evaluation Activities
ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.2.1.1 TSS Activity
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.	6.2.1.1 TSS Activity

Table 2: Mapping of ADV_FSP.1 CEM Work Units to Evaluation Activities

6.2.1.1 TSS Activity:

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

The evaluator shall confirm identification information of the TSFI associated with the SFR described in the TSS and confirm the consistency with the description related to each interface.

The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on identification information of the TSFI in the TSS description as well as on the information of purposes, methods of use, and parameters for each TSFI in the guidance documents.

*The assurance activities specific to each SFR are described in Section 2, and also applicable SFRs from Appendix B, Appendix C, and Appendix D, and the evaluator **shall** perform evaluations by adding to this assurance component.*

Evaluator Assessment:

The evaluator confirms that the identifiable external interfaces are identified in the TSS. The SFRs are mapped to the TSFI appropriately. The information regarding the external interfaces comes from the guidance documents, the FSP and the TSS. The TSFI are: Power, Touch Screen, Network, GUI Management, and PKI Card Reader.

6.3 AGD: Guidance Documents

The guidance documents will be provided with the developer's security target. Guidance must include a description of how the administrator verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an administrator.

Guidance must be provided for every Operational Environment that the product supports as claimed in the ST. This guidance includes:

- instructions to successfully install the TOE in that environment; and

- instructions to manage the security of the TOE as a product and as a component of the larger Operational Environment.

Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified in Section 4, and applicable assurance activities in Appendix B, Appendix C, and Appendix D.

6.3.1 AGD_OPE.1 Operational User Guidance

CEM AGD_OPE.1 Work Units	Evaluation Activities
AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.3.1.1 Operational Guidance Activity

Table 3: Mapping of AGD_OPE.1 CEM Work Units to Evaluation Activities

6.3.1.1 Operational Guidance Activity:

The contents of operational guidance are confirmed by the assurance activities in Section 4, and applicable assurance activities in Appendix B, Appendix C, and Appendix D, and the TOE evaluation in accordance with the CEM.

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

Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

Evaluator Assessment:

The guidance documents were evaluated as per the CEM and the assurance activities. All pertinent information was in the guidance documents which was comprised of the Administrator Guide, relevant user guides, the CC supplement and the Embedded Web Server document. They contain the information required in Appendices A, B, C and D.

6.3.2 AGD_PRE.1 Preparative Procedures

CEM AGD_PRE.1 Work Units	Evaluation Activities
AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.3.2.1 Operational Guidance Activity
AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.	6.3.2.1 Operational Guidance Activity

Table 5: Mapping of AGD_PRE.1 CEM Work Units to Evaluation Activities

6.3.2.1 Operational Guidance Activity

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

Evaluator Assessment:

The guidance documentation was available for every printer platform.

6.4 ALC: Life-Cycle Support

At the assurance level provided for the TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for the evaluation at this assurance level.

6.4.1 ALC_CMC.1 Labeling of the TOE

CEM ALC_CMC.1 Work Units	Evaluation Activities
ALC_CMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.4.1.1 Operational Guidance Activity

Table 6: Mapping of ALC_CMC.1 CEM Work Units to Evaluation Activities

6.4.1.1 Operational Guidance Activity

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.

Evaluator Assessment:

The printer identifiers were unique, they were displayed on the hardware and were available through the menu pages of the printer. The versions were consistent with those in the [ST].

6.4.2 ALC_CMS.1 TOE CM Coverage

Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1

CEM ALC_CMS.1 Work Units	Evaluation Activities
ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.4.2.1 Operational Guidance Activity

Table 7: Mapping of ALC_CMS.1 CEM Work Units to Evaluation Activities

6.4.2.1 Operational Guidance Activity

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.

Evaluator Assessment:

The TOE is uniquely identified, and this identification was the same in the user manuals and the [ST]. There was no ambiguity.

6.5 ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces as constrained by the availability of design information presented in the TSS. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

6.5.1 ATE_IND.1 Independent Testing – Conformance

CEM ATE_IND.1 Work Units	Evaluation Activities
ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.5.1.1 Test Activity
ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.	6.5.1.1 Test Activity

Table 8: Mapping of ATE_IND.1 CEM Work Units to Evaluation Activities

6.5.1.1 Test Activity

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the product models to be test, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that 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 or the functionality by the TOE.

This 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.*

Evaluator Assessment:

The evaluator devised a test plan to test representative models. An equivalence argument as to why the printer could be used as a representative of the group was presented with the eligibility package.

The test plan has objectives, expected results and actual results. The tests that were performed covered all of the test assurance activities.

6.6 AVA: Vulnerability Assessment

For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

6.6.1 AVA_VAN.1 Vulnerability Survey

CEM AVA_VAN.1 Work Units	Evaluation Activities
AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	6.6.1.1 Test Activity
AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.	6.6.1.1 Test Activity
AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing basic attack potential	6.6.1.1 Test Activity

Table 9: Mapping of AVA_VAN.1 CEM Work Units to Evaluation Activities

6.6.1.1 Test Activity

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in printing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report.

For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by

assessing the attack vector needed to take advantage of the vulnerability.

For example, if the vulnerability can be detected by pressing a 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.

Evaluator Assessment:

A vulnerability search of the National Vulnerability Database (https://nvd.nist.gov/vuln/search) and the developer's site (https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html) was conducted The search was performed with the following search terms: Lexmark, Lexmark Multi-Function Printer, CX730, CX930, CX931, MX931, CXTPC, CXTMM, MXTPM, 081.234, Infineon OPTIGA Trusted Platform Module, Infineon OPTIGA TPM, SLB9672 2.0, PCL 5e, PCL 6, PPDS, PostScript 3, PDF 1.7, Direct Image, AirPrint, apache 2.4.52, apr 1.7.0, apr-util, ethtool 5.4, expat 2.2.9, freetype 2.10.1, Iproute2 5.5.0, iptables 1.8.4, openssh 8.2p1, openssl 1.1.1l, openssl 1.0.2, openssl-fips 2.0.12, panel-apps, panel-drivers, panel-headers, panel-libs, strongswan 5.7.1, stunnel 5.57, and usbutils 012.

No vulnerabilities that would impact the evaluated configuration were found.