Assurance Activity Report for Lexmark CX725h and XC4150 Multi-Function Printers against the Protection Profile for Hardcopy Devices

Version 1.1
1 March 2018

Prepared by:
EWA-Canada

Prepared for:
Communications Security Establishment (CSE) and
National Information Assurance Partnership (NIAP)

Contents

1 Introduction

This document presents assurance activity evaluation results of Target of Evaluation (TOE). There are three types of assurance activities included.

1. TOE Summary Specification (TSS) - An indication that the required information is in the TSS section of the Security Target;

2. Guidance Documentation - 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 documents were consulted:

[CC_Supp], Lexmark™ Common Criteria Installation Supplement and Administrator Guide, February 2018.

[CL], Lexmark Multi-Function Printers with Hard Drives Configuration Item List, Version 1.4, February 27, 2018.

[CX725_CX727_User's_Guide], Lexmark™ CX725, CX727 User's Guide, June 2017.

[EAR], Lexmark Entropy Assessment Report, Version 1.3, December 12, 2017.

[ETProcRes], Evaluation Test Plan, Procedures and Test Results for Common Criteria Evaluation of Lexmark CX725h and XC4150 Multi-Function Printers, Version 0.2, January 24, 2018.

[ETR], Evaluation Technical Report for the Protection Profile for Hardcopy Devices Common Criteria Evaluation of Lexmark International, Inc.'s Lexmark CX725h and XC4150 Multi-Function Printers, Version 1.1, 1 March 2018.

[EWS_Admin_Guide], Lexmark™ Embedded Web Server - Security Administrator's Guide, June 2017.

[FSP], Lexmark Multi-Function Printers with Hard Drives Functional Specification, Version 1.1, October 6, 2017.

[KMD], Lexmark Key Management Description, Version 1.2, January 10, 2018.

[Menus_Guide], Lexmark™ Menus Guide, August 2017.

[PP_HCD], Protection Profile for Hardcopy Devices, Version 1.0, September 10, 2015.

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

[SP], Lexmark™ Crypto-Module, FIPS 140-2 Non-Proprietary Security Policy Level 1 Validation, Version 1.5, July 2015.

[ST], Lexmark CX725h and XC4150 Multi-Function Printers Security Target, Version 1.7, February 27, 2018.

[XC4100_User's_Guide], Lexmark™ XC4100 Series User's Guide, December 2016.

1.2 Technical Decisions for the Protection Profile for Hardcopy Devices

TD0074: FCS_CKM.1(a) Requirement in HCD PP v1.0
TD0157: FCS_IPSEC_EXT.1.1 - Testing SPDs
TD0176: FDP_DSK_EXT.1.2 - SED Testing
TD0219: NIAP Endorsement of Errata for HCD PP v1.0
TD0253: Assurance Activities for Key Transport
TD0261: Destruction of CSPs in flash

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 have been extracted from Protection Profile for Hardcopy Devices [PP_HCD].

2.1 Class FAU: Security Audit

2.1.1 FAU_GEN.1 Audit Data Generation

2.1.1.1 Application Note:

In cases where user identification events are inseparable from user authentication events, they may be considered to be a single event for audit purposes.

Regarding FMT_SMR.1, if the relationship between users and roles is not modifiable, its auditable event cannot be generated and the requirement to generate an audit record can be ignored.

The ST author can include other auditable events directly in the table; they are not limited to the list presented.

Assurance Activity:

2.1.1.2 TSS 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 Comment:

The TSS describes the following:

The auditable events described in the TSS 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 in section 6.1.1.1 is provided. The required severity level for audit logs is indicated in Section 7.1.6 of the [ST].

2.1.1.3 Operational Guidance 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 Comment:

*Section **Audit log** in the [CC_Supp] 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 Started (and source IP address for print jobs);*

- *Successful user identification and authentication: Recorded information includes Username and Login successful (and source IP for address for remote users);*
- *Unsuccessful user authentication: Recorded information includes Login failed with supplied user ID (and source IP for address for remote users);*
- *Unsuccessful user identification: Recorded information includes Login failed with supplied user ID (and source IP for address for remote users);*
- *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; and*
- *Audit log cleared by an authorized administrator: Recorded information includes confirmation of audit log being cleared.*

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

2.1.1.4 Test Activity:

The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 1 is appropriately generated.
2. The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods.
3. The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.

Evaluator Comment:

Throughout performing testing, the evaluator ensured that the audit record of each of the auditable events described in Table 1 in the [PP_HCD] was appropriately generated. This included testing that involved the following scenarios:

a. *Job start/completion (i.e., print jobs, fax jobs, etc.);*
b. *Use of management functions (i.e., changing security settings);*
c. *Clearing the audit log;*
d. *Modifying user permissions; and*
e. *Successful and unsuccessful authentication/identification attempts.*

The evaluator checked a representative sample for generating auditable events on two interfaces of the TOE – 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), LDAP, Kerberos, and SmartCard.

The test steps that the evaluator performed to execute this test are described in [ETProcRes], section 4.2.1. Additional auditable events were generated via other tests in the [ETProcRes].

2.1.2 FAU_GEN.2 User Identity Association

Assurance Activity:

The Assurance Activities for FAU_GEN.1 address this SFR.

2.1.3 FAU_SAR.1 Audit Review

The following assurance activities are required when storing audit records inside the TOE.

Assurance Activity:

2.1.3.1 TSS 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 Comment:

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.

2.1.3.2 Operational Guidance Activity:

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

Evaluator Comment:

*Section **Configuring security audit log settings** in the [EWS_Admin_Guide] states that security logs are stored on the device and may also be transmitted to a syslog server. Section **Audit log** in the [CC_Supp] document mentions that the security log can also be exported through e-mail or browsed.*

2.1.3.3 Test 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 retrieving audit records.

Evaluator Comment:

The evaluator confirmed that the audit record is provided as specified in the operational guidance by retrieving the audit records via the TOE's 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 this test are described in [ETProcRes], sections 4.2.2 and 4.2.3. The actual results met the expected results.

2.1.4 FAU_SAR.2 Restricted Audit Review

Assurance Activity:

2.1.4.1 Test Activity:

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

2.1.5 FAU_STG.1 Protected Audit Trail Storage

Assurance Activity:

2.1.5.1 TSS 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 Comment:

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.

2.1.5.2 Operational Guidance 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 from unauthorized access (modification, deletion) are consistent.

Evaluator Comment:

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 to be used for communication. Only administrators with the Security Menu permission may upload the audit log in syslog or CSV format using their browser and clear the audit log.

There is no mechanism to modify audit records.

This information from the TSS is consistent with that in sections ***Setting up Internet Protocol Security (IPSec)*** *and* ***Configuring security audit logging*** *in the [CC_Supp] document and in section* ***Configuring security audit log settings*** *in the [EWS_Admin_Guide].*

2.1.5.3 Test Activity:

The evaluator shall also perform the following test:

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 Comment:

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], sections 4.2.2 and 4.2.3. The actual results met the expected results.

2.1.6 FAU_STG.4 Prevention of Audit Data Loss

Assurance Activity:

The following assurance activities are required when storing audit records inside the TOE.

2.1.6.1 TSS 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 Comment:

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.

2.1.6.2 Operational Guidance 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 Comment:

*Section **Configuring security audit logging** in the [CC_Supp] document and section **Configuring security audit log settings** in the [EWS_Admin_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.*

2.1.6.3 Test 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 Comment:

The evaluator performed testing which caused auditable events to be generated after the capacity of audit records on the TOE became full. The evaluator verified that an e-mail alert is sent after the audit log reaches the set percentage of its capacity. The evaluator confirmed that the oldest records were overwritten when the audit log reached near-full capacity. The test steps that the evaluator performed to execute this test are described in [ETProcRes] section 4.2.4. The actual results met the expected results.

2.1.7 FAU_STG_EXT.1 Extended: External Audit Trail Storage

Assurance Activity:

2.1.7.1 TSS 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 Comment:

Audit data is transferred to an external audit server over IPsec. The TSS does not indicate the amount of audit data that is stored locally. When the audit log storage reaches 98% capacity, the oldest records are

purged until the used space is lowered to 80% capacity. Audit data is stored in the internal log as it is generated. Audit logs are sent to the syslog server when the transfer is initiated by the administrator. The internal logs are removed when the administrator initiates removal, or when the log storage reached 98% capacity. Audit capabilities are discussed in Section 7.1.6 of the [ST].

Section 7.1.6 of the [ST] now indicates that the internal audit log storage is 1MB.

2.1.7.2 Operational Guidance 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. The evaluator shall perform the following test for this requirement:

Evaluator Comment:

*Section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] 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 section **Configuring security audit logging** in the [CC_Supp] document and in section **Configuring security audit log settings** in the [EWS_Admin_Guide].*

2.1.7.3 Test Activity:

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 Comment:

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 so as to witness a large amount of audit data being transferred.

The evaluator confirmed using Wireshark version 2.4.1 that the data is not viewable in the clear during this transfer, and confirmed that the data is successfully received by the audit server. For this test, the evaluator configured a CentOS Linux 7 machine to use rsyslog version 8.30.0 for receiving audit records from the TOE. The actual results met the expected results for this test.

2.2 Class FCS: Cryptographic Support

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

2.2.1.1 Application Note:

The ST author selects the key generation scheme used for key establishment and device authentication. If multiple schemes are supported, then the ST author should iterate this component to capture this capability. When key generation is used for device authentication, the public key is expected to be associated with an X.509v3 certificate. If the TOE acts as a receiver in the RSA key establishment scheme, the TOE does not need to implement RSA key generation.

Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is not expected that the TOE will generate domain parameters, and therefore there is no additional domain parameter validation needed when the TOE complies with the protocols specified in this PP.

SP 800-56B references (but does not mandate) key generation according to FIPS 186-3. For purposes of compliance in this version of the HCD PP, RSA key pair generation according to FIPS 186-4 is allowed in order for the TOE to claim conformance to SP 800-56B.

The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, “Recommendation for Key Management” for information about equivalent key strengths.

Assurance Activity:

2.2.1.2 TSS Activity:

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 Comment:

Table 21 in [ST] Section 7.1.4 indicates how the TSF complies with 800-56B. Each shall and should statement is implemented, including those in Section 6 related to RSA key establishment.

2.2.1.3 Test Activity:

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 Comment:

The above test activity was satisfied through the Cryptographic Algorithm Validation Program (CAVP). The implemented RSA key generation was verified as meeting FIPS 186-4 using the “The 186-4 RSA Validation System (RSA2VS)”. The TOE generates 2048 bit RSA keys having an equivalent symmetric key strength of 112 bits. The RSA implementation was awarded RSA validation certificate 2695:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/RSA#2695

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

2.2.2.1 Application Note:

Symmetric keys may be used to generate keys along the key chain.

Assurance Activity:

2.2.2.2 TSS Activity:

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

Evaluator Comment:

The functionality described in FCS_RBG_EXT.1 is invoked when the disk encryption functionality is enabled during installation. This is described in Sections 7.1.3 and 7.1.4 of the [ST].

2.2.2.3 KMD 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 to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

The KMD is described in Appendix F.

Evaluator Comment:

Section 2. Key Management Description in the [KMD] specifies the function call used when calling the third-party DRBG function.

FCS_COP.1(d) in section 6.1.2.7 FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption) in the [ST] specifies an AES key size of 256 bits and an AES mode of CBC to be used for the encryption/decryption of user data.

Section 2. Key Management Description in the [KMD] describes the parameters used when calling the third-party DRBG function and provides a description of the vendor's assumption for the amount of entropy seeding the third-party DRBG.

2.2.3 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

2.2.3.1 Application Note:

"Cryptographic Critical Security Parameters" are defined in FIPS 140-2 as "security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module".

Keys, including intermediate keys and key material that are no longer needed are destroyed by using an approved method, FCS_CKM.4.1. Examples of keys are intermediate keys, submasks, and BEV. There may be instances where keys or key material that are contained in persistent storage are no longer needed and require destruction. Based on their implementation, vendors will explain when certain keys are no longer needed. There are multiple situations in which key material is no longer necessary, for example, a wrapped key may need to be destroyed when a password is changed. However, there are instances when keys are allowed to remain in memory, for example, a device identification key.

Assurance Activity:

2.2.3.2 TSS 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 then should be expected to be destroyed.

Evaluator Comment:

The disk encryption key is destroyed if the disk encryption functionality is disabled. Session keys are destroyed when the session is terminated. 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 Table 16 indicates that the passwords are destroyed in flash when the account is deleted. Passwords in memory are destroyed at the conclusion of the login.

2.2.3.3 KMD 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 Comment:

Section 2. Key Management Description in the [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 description of the key material destruction in the [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 or overwriting memory locations with zeros 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 Application Note:

In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on whether they are in volatile memory or non-volatile memory within the TOE.

The selection of block erase for non-volatile memory applies only to flash memory.

Within the selections is the option to overwrite the memory location with a new value of a key. The intent is that a new value of a key (as specified in another SFR within the PP) can be used to "replace" an existing key.

Several selections allow assignment of a 'value that does not contain any CSP'. This means that the TOE uses some other specified data not drawn from a source that may contain key material or reveal information about key material, and not being any of the particular values listed as other selection options. The point of the phrase 'does not contain any CSP' is to ensure that the overwritten data is carefully selected, and not taken from a general 'pool' that might contain current or residual data that itself requires confidentiality protection.

Assurance Activity:

2.2.4.2 TSS Activity:

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 Comment:

Table 19 - 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 zeroes are used to overwrite cryptographic keys. Section 7.1.4 Trusted Communications in the TSS states that "The TOE zeroizes the session keys by overwriting once with zeros when the sessions are terminated. Any copy of an RSA private key or PSK in RAM is destroyed when power is turned off or by overwriting with zeroes when the buffer holding it is released." Section 7.1.10 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.

2.2.4.3 KMD Activity:

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.

Evaluator Comment:

Section 2. Key Management Description in the [KMD] describes how keys are managed in volatile memory or RAM.

Section 2. Key Management Description in the [KMD] lists each type of key that is stored in nonvolatile memory, and identifies the memory types where key material is stored.

Section 2. Key Management Description in the [KMD] describes the interfaces that are used to service commands to read/write memory.

2.2.4.4 Operational Guidance Activity:

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 Comment:

Section 7.1.10 Common Functionality Regarding Key Destruction in Flash Memory in the [ST] specifies that "The flash component supports the TRIM command and implements garbage collection to destroy the persistent copies of the old storage locations when not actively engaged in other tasks. The file system that maps to the flash component, and on which these keys are stored, also supports the TRIM command and the file system is configured to use it."

2.2.4.5 Test Activity:

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

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

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

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

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

Test 2: Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)

2. Cause the TOE to clear the key.

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

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 Comment:

The evaluator witnessed developer testing 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 witnessed by the evaluator are detailed in [ETProcRes] section 4.2.5. Tests 1 through 4 were successful. The actual results met the expected results.

2.2.5 FCS_COP.1(a) Cryptographic Operation (Symmetric Encryption/Decryption)

2.2.5.1 Application Note:

For the assignment, the ST author should assign the mode or modes in which AES operates to support the cryptographic protocols chosen for FTP_ITC and FTP_TRP.

For the selection, the ST author should choose the standards that describe the modes specified in the assignment.

Assurance Activity:

2.2.5.2 Test 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 Comment:

The above test activity was satisfied through the CAVP. The implemented AES encryption and decryption uses the CBC mode of operation. It was verified using "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)". The user and kernel AES implementations were awarded AES validation certificates 4997 and 4851:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/AES#4997 and
https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/AES#4851

2.2.6 FCS_COP.1(b) Cryptographic Operation (for Signature Generation/Verification)

2.2.6.1 Application Note:

The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

For elliptic curve-based schemes, the key size refers to the log2 of the order of the base point.

Assurance Activity:

2.2.6.2 Test 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 Comment:

The above test activity was satisfied through the CAVP. The implemented RSA signature generation and verification was verified as meeting FIPS 186-4 using the "The 186-4 RSA Validation System (RSA2VS)". The TOE generates 2048 bit RSA keys. The RSA implementation was awarded RSA validation certificate 2695:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/RSA#2695

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

2.2.7.1 Application Note (for O.STORAGE_ENCRYPTION):

The hash selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(d). (SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The selection of the standard is made based on the algorithms selected.

Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP 800-131A.

Assurance Activity:

2.2.7.2 TSS 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 Comment:

The association of hash functions with other TSF cryptographic functions is documented in the TSS in the [ST] as follows:

- *Section 7.1.4 Trusted Communications states that SHA-256 and SHA-384 are supported for HMACs, that PSKs are conditioned using SHA-1, SHA-256, or SHA-384, and that SHA-1, SHA-256, or SHA-384 is used in the SA exchange; and*

- *Section 7.1.7 Trusted Operation states that SHA256 is used for the digital signature for executable code integrity and that a SHA256 hash is maintained for each executable page during operation.*

2.2.7.3 Operational Guidance 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 Comment:

*Configuration for optional hash sizes is discussed in section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide].*

2.2.7.4 Test 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 $1 \leq i \leq m$. For SHA-512, the length of the i-th message is 1024 + 99*i, where $1 \leq i \leq m$. 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 Comment:

The above test activity was satisfied through the CAVP. The claimed hash algorithms of SHA-1, SHA-256, and SHA-384 were verified using "The Secure Hash Algorithm Validation System (SHAVS)". The user and kernel hash algorithm implementations were awarded SHA validation certificates 3990 and 4063:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/SHS#3990 and
https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/SHS#4063

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

2.2.8.1 Application Note:

This PP allows for software encryption or hardware encryption.

If XTS Mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619. XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS mode are selected.

The intent of this requirement is to specify the approved AES modes that the ST Author may select for AES encryption of the appropriate information on the Field-Replaceable Nonvolatile Storage Device. For the first selection, the ST author should indicate the mode or modes supported by the TOE implementation. The second selection indicates the key size to be used, which is identical to that specified for FCS_CKM.1(b). The third selection must agree with the mode or modes chosen in the first selection. If multiple modes are supported, it may be clearer in the ST if this component was iterated.

Assurance Activity:

2.2.8.2 TSS Activity:

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

Evaluator Comment:

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

2.2.8.3 Operational Guidance 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 Comment:

Only the CBC mode of AES with 256-bit keys is supported for disk encryption so no configuration by the end user is needed.

2.2.8.4 Test 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 from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

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

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

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 AES- CBC-Decrypt.

AES-GCM Test

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

128 bit and 256 bit keys

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

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

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

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

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

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

XTS-AES Test

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

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

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

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

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

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

Evaluator Comment:

The above test activity was satisfied through the CAVP. The implemented AES encryption and decryption in the CBC mode of operation was tested with the four KATs, the Multi-Block Message Test, and the Monte Carlo Test following "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)". The AES user and kernel implementations were awarded AES validation certificates 4997 and 4851:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/AES#4997 and
https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/AES#4851

2.2.9 FCS_COP.1(g) Cryptographic Operation (for Keyed-Hash Message Authentication)

Assurance Activity:

2.2.9.1 Test 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 Comment:

The above test activity was satisfied through the CAVP. The claimed HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384 were tested following "The Keyed-Hash Message Authentication Code Validation System (HMACVS)". The HMAC implementation was awarded HMAC validation certificate 3248:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/HMAC#3248

2.2.10 FCS_IPSEC_EXT.1.1

2.2.10.1 Application Note:

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rulesets, a "traditional" SPD, etc. Regardless of the implementation details, there is a notion of a "rule" that a packet is "matched" against and a resulting action that takes place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

Assurance Activity:

2.2.10.2 TSS Activity:

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.

Evaluator Comment:

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.

2.2.10.3 Operational Guidance Activity:

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.

Evaluator Comment:

*Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] and section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] discuss the configuring of Security Associations (SAs).*

2.2.10.4 Test Activity:

The evaluator uses the operational guidance 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.

Evaluator Comment:

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 [ETProcRes] section 4.2.22. The actual results met the expected results.

2.2.11 FCS_IPSEC_EXT.1.2

Assurance Activity:

2.2.11.1 TSS Activity:

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).

Evaluator Comment:

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

2.2.11.2 Operational Activity:

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

Evaluator Comment:

Only transport mode is available. The instructions in sections ***Configuring IP Security (IPsec) settings*** *in the [EWS_Admin_Guide] and section* ***Setting up Internet Protocol Security (IPSec)*** *in the [CC_Supp] discuss the configuration of connections.*

2.2.11.3 Test Activity:

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.

Evaluator Comment:

The evaluator performed testing to confirm that the TOE is able to initiate a connection with an IPsec Peer using transport mode. Throughout the testing documented in [ETProcRes], all external IT entities connecting to the TOE used transport mode with a variety of the allowed cryptographic algorithms, authentication methods, and other configuration parameters to ensure that an allowable SA can be negotiated. The evaluator observed via captured packets in Wireshark 2.4.1 that successful connections were established using transport mode.

2.2.12 FCS_IPSEC_EXT.1.3

Assurance Activity:

2.2.12.1 TSS Activity:

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.

Evaluator Comment:

Section 7.1.4 of the [ST] indicates that packets are processed against the SPD, and describes the rules that are implemented. Incoming packets from authorized addresses are accepted and all other IP datagrams are discarded.

2.2.12.2 Operational Guidance Activity:

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.

Evaluator Comment:

*Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] and section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] discuss the configuring of SAs for the SPD.*

2.2.12.3 Test Activity:

The evaluator shall perform the following test:

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

Evaluator Comment:

This test activity is not applicable to the TOE as the SPD does not have the capability to apply a BYPASS rule. The evaluator has ensured that packets are not permitted to flow to any of the TOE's interfaces if they do not match the PROTECT rule.

2.2.13 FCS_IPSEC_EXT.1.4

Assurance Activity:

2.2.13.1 TSS Activity:

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).

Evaluator Comment:

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

2.2.13.2 Operational Guidance Activity:

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.

Evaluator Comment:

*Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] discusses the setting of the Proposed Authentication Method for IPSec.*

2.2.13.3 Test Activity:

The evaluator shall also perform the following test:

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.

Evaluator Comment:

The evaluator configured the TOE as indicated in the operational guidance to use each of the selected algorithms, and attempted to establish a connection using ESP. The following algorithms were used by an IPsec Peer to successfully connect to the TOE:

a. *aes256-sha1-modp2048*
b. *aes256-sha256-modp2048s256*
c. *aes256-sha384-modp2048s256*
d. *aes256-sha256-modp2048*
e. *aes256-sha384-modp2048*
f. *aes128-sha256-modp2048s256*
g. *aes128-sha1-modp2048*
h. *aes128-sha256-modp2048*

The test steps that the evaluator performed to execute this test are detailed in [ETProcRes] section 4.2.24. The actual results met the expected results.

2.2.14 FCS_IPSEC_EXT.1.5

2.2.14.1 Application Note:

Either IKEv1 or IKEv2 support must be provided, although conformant TOEs can provide both; the first selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4304 identifies support for extended sequence numbers, which compliant TOEs can specify using the second selection. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used.

Assurance Activity:

2.2.14.2 TSS Activity:

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

Evaluator Comment:

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

2.2.14.3 Operational Guidance Activity:

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.

Evaluator Comment:

*Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] and section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] discuss the configuration of the TOE to use either IKEv1 or IKEv2.*

2.2.14.4 Test Activity:

(conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.

Evaluator Comment:

This test is not applicable to the evaluation. As per the [Errata1_HCD], it is not required for the TOE to perform NAT traversal if IKEv2 is selected. NAT traversal is not claimed in this SFR.

2.2.15 FCS_IPSEC_EXT.1.6

Assurance Activity:

2.2.15.1 TSS Activity:

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES- CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Evaluator Comment:

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

2.2.15.2 Operational Guidance Activity:

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.

Evaluator Comment:

*Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] discusses the setting of DH (Diffie-Hellman) Group Proposal, Proposed Encryption method, and Proposed Authentication Methods for IPSec.*

2.2.15.3 Test Activity:

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.

Evaluator Comment:

The evaluator configured the TOE to use each ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which was configured to only accept the payload encrypted using the indicated ciphersuites. The following ciphersuites were used by an IPsec Peer to successfully connect to the TOE:

a. *aes256-sha1-modp2048*
b. *aes256-sha256-modp2048s256*
c. *aes256-sha384-modp2048s256*
d. *aes256-sha256-modp2048*
e. *aes256-sha384-modp2048*
f. *aes128-sha256-modp2048s256*
g. *aes128-sha1-modp2048*
h. *aes128-sha256-modp2048*

These ciphersuites were tested using both IKEv1 and IKEv2 to confirm that a connection could be established using either IKE version. The test steps that the evaluator performed to execute this test are detailed in [ETProcRes] section 4.2.24. The actual results met the expected results.

2.2.16 FCS_IPSEC_EXT.1.7

Assurance Activity:

2.2.16.1 TSS Activity:

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.

Evaluator Comment:

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

2.2.16.2 Operational Guidance Activity:

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.

Evaluator Comment:

The mode does not require configuration of the TOE prior to its operation so no instructions in the operational guidance are required.

2.2.16.3 Test Activity:

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.

Evaluator Comment:

The evaluator confirmed that a connection using IKEv1 Phase 1 connection in aggressive mode shall fail. The evaluator configured an IPsec Peer to attempt to establish a connection using IKEv1 Phase 1 aggressive mode. The connection could not be established in aggressive mode. The test steps performed by the evaluator for this test are detailed in [ETProcRes] section 4.2.25.

2.2.17 FCS_IPSEC_EXT.1.8

2.2.17.1 Application Note:

The ST Author is afforded a selection based on the version of IKE in their implementation. If the lifetime limitations are configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance.

As far as SA lifetimes are concerned, the TOE can limit the lifetime based on the number of bytes transmitted, or the number of packets transmitted. Either packet-based or volume-based SA lifetimes are acceptable; the ST author makes the appropriate selection to indicate which type of lifetime limits are supported.

Assurance Activity:

2.2.17.2 Operational Guidance Activity:

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."

Evaluator Comment:

*Section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] describes how to configure SA lifetimes. Time-based limits are supported with values for Phase 1 SAs (IKE SA Lifetime (Hours) menu) allowed to be up to 24 hours and to 8 hours for Phase 2 SAs (IPSec SA Lifetime (Hours) menu).*

2.2.17.3 Test Activity:

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.

Evaluator Comment:

The evaluator constructed a test where a Phase 1 SA was established and attempted to be maintained for more than 24 hours before it was renegotiated. The evaluator configured the TOE to maintain the Phase 1 SA for 24 hours, and configured an IPsec peer to maintain the Phase 1 SA for 25 hours. The evaluator observed that the SA was renegotiated in less than 24 hours.

The evaluator repeated this test in a similar fashion for Phase 2 SAs, except that the lifetime was 8 hours instead of 24. The evaluator observed that the SA was renegotiated in less than 8 hours.

The test steps that the evaluator performed for this test are detailed in [ETProcRes] section 4.2.26.

2.2.18 FCS_IPSEC_EXT.1.9

2.2.18.1 Application Note:

The above requires that the TOE support DH Group 14. If other groups are supported, then those should be selected (for groups 24, 19, 20, and 5) or specified in the assignment above; otherwise "no other DH groups" should be selected. This applies to IKEv1/IKEv2 exchanges.

Assurance Activity:

2.2.18.2 TSS Activity:

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.

Evaluator Comment:

Section 7.1.4 of the [ST] indicates that groups 14 and 24 may be used, and indicates how the DH group is negotiated with the peer.

2.2.18.3 Test Activity:

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

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

Evaluator Comment:

The evaluator performed tests to ensure that for both Diffie-Hellman groups 14 and 24, connections via IKEv1 and IKEv2 protocols were successfully established. The test steps performed by the evaluator for this test are detailed in [ETProcRes] section 4.2.24.

2.2.19 FCS_IPSEC_EXT.1.10

2.2.19.1 Application Note:

The selected algorithm should correspond to an appropriate selection for FCS_COP.1(b). If IPsec is included in the TOE, the ST author also includes FIA_PSK_EXT from Appendix D.2.6.

Assurance Activity:

2.2.19.2 TSS Activity:

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 Comment:

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 specified in the requirement.

2.2.19.3 Test Activity:

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 Comment:

The evaluator ran tests to ensure that all IKE protocols perform Peer authentication using the RSA algorithm and Pre-shared keys. Using an IPsec Peer, the evaluator verified that IPsec sessions can be established with the TOE using:

a. *The RSA algorithm for certificate-based authentication; or*
b. *Pre-shared keys.*

Throughout testing, multiple external IT entities were configured using both of the above methods. The test steps performed by the evaluator for this test activity are also detailed in [ETProcRes] sections 4.2.22 to 4.2.26. The actual results met the expected results.

2.2.20 FCS_KYC_EXT.1 Extended: Key Chaining

2.2.20.1 Application Note:

This SFR forms a keychain that terminates either with a DEK or a BEV to unlock a self-encrypting drive. If passwords are not used, it can be a keychain of one, with no intermediate keys forming the DEK or BEV, provided that key is protected. For example, if the DEK for an SED is not stored on the SED and is released on power-up, a keychain of one is allowed.

Key Chaining is the method of using multiple layers of encryption keys to ultimately secure the BEV (Border Encryption Value). The number of intermediate keys will vary – from one (e.g., taking the conditioned password authorization factor and directly using it as the BEV) to many. This applies to all keys that contribute to the ultimate wrapping or derivation of the BEV; including those in areas of protected storage (e.g. TPM stored keys, comparison values).

Multiple key chains to the BEV are allowed, as long as all chains meet the key chain requirement.

Once the ST Author has selected a method to create the chain (either by unwrapping or encrypting keys), they pull the appropriate requirement out of this appendix. It is allowable for an implementation to use for any or all methods.

The method the TOE uses to chain keys and manage/protect them is described in the Key Management Description; see Key Management Description for more information.

Assurance Activity:

2.2.20.2 TSS 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 Comment:

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

2.2.20.3 KMD 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 Comment:

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

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

2.2.21.1 Application Note:

ISO/IEC 18031:2011 contains different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used and include the specific underlying cryptographic primitives used in the requirement. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. Table C.2 in ISO/IEC 18031:2011 provides an identification of Security strengths, Entropy and Seed length requirements for the AES-128 and 256 Block Cipher.

The CTR_DRGB in ISO/IEC 18031:2011 requires using derivation function, whereas NIST SP 800-90A does not. Either model is acceptable. In the first selection in FCS_RBG_EXT.1.1, the ST Author chooses the standard with which they are compliant.

The first selection in FCS_RBG_EXT.1.2 the ST author fills in how many entropy sources are used for each type of entropy source they employ. It should be noted that a combination of hardware and software based noise sources is acceptable.

It should be noted that the entropy source is considered to be a part of the RBG and if the RBG is included in the TOE, the developer is required to provide the entropy description outlined in Appendix E. The documentation *and tests* required in the Evaluation Activity for this element necessarily cover each source indicated in FCS_RBG_EXT.1.2.

Assurance Activity:

2.2.21.2 TSS 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 Comment:

Entropy is provided 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]. The DRBG collects entropy bits from the Lexmark Secure Element as needed. This is described in the [KMD] document.

A full description of the processing of the output of the third-party source is discussed in the [EAR] and in the [KMD] documents.

2.2.21.3 Entropy Description 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 Comment:

The [EAR] provides all of 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.

2.2.21.4 Operational Guidance 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 Comment:

The Lexmark Secure Element (P/N 57X0085) needs to be installed in the TOE. Instructions for installing the Lexmark Secure Element come with the part.

2.2.21.5 Test 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 Comment:

The above test activity was satisfied through the CAVP. The DRBG is a CTR_DRBG using AES. It was tested following "The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS)". The DRBG implementation was awarded DRBG validation certificate 1820:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DRBG#1820

2.3 Class FDP: User Data Protection

2.3.1 Application Note:

The User Data Access Control SFP is composed of Table 2, Table 3, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, and FMT_MSA.3.

2.3.2 FDP_ACC.1 Subset Access Control

Assurance Activity:

2.3.2.1 Assurance Activity:

It is covered by assurance activities for FDP_ACF.1.

Evaluator Comment:

See Section 2.3.3.

2.3.3 FDP_ACF.1 Security Attribute Based Access Control

2.3.3.1 Application Note:

In general, the ST Author may modify this SFP provided that any changes are more restrictive. As examples, the ST Author may: remove the rules related to Document Processing functions that are not present in a TOE, add or modify rules to further deny access, or subdivide User Data to further restrict access for some data (e.g., D.USER.JOB.PROT and D.USER.JOB.CONF). Empty cells in the table indicate that the operation may be permitted, but it is not required to be permitted.

In particular, referring to Table 2 and Table 3:

- A cell marked "Denied" indicates that the user (row) must not be permitted to perform the operation (column). The ST Author cannot override this.
- A cell that is blank indicates that the user may be permitted to perform the operation. However, the ST author may add conditions or restrictions, or deny permission entirely.

- A cell that is marked with a Condition means that the user can be permitted to perform the operation, provided that it meets that Condition as specified below. As with blank cells, the ST author can make it more restrictive.

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

See also the following Notes that are referenced in Table 2 and Table 3:

Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.

Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.

Note 3: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.

Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.

Assurance Activity:

2.3.3.2 TSS Activity:

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

Evaluator Comment:

Section 7.1.2 of the [ST] describes the functions required to realize the Print, Scan, Copy, Fax Send and Fax Receive capabilities.

2.3.3.3 Operational Guidance Activity:

The evaluator shall check to ensure that the operational guidance contains a description of the operation to realize the SFP defined in Table 2 and Table 3, which is consistent with the description in the TSS.

Evaluator Comment:

*Section **Fax** in the [Menus_Guide] describes the operations related to the parameters to realize the SFP.*

2.3.3.4 Test 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 representative sets of the object types defined in Table 2 and Table 3 (including some cases where operations are either permitted or denied)
- representative sets for the combinations of the setting for security attributes that are used in access control

Evaluator Comment:

The evaluator performed tests to ensure that the functions to realize the SFP defined in Table 2 and Table 3 with each type of interface (operation panel, embedded web server) to the TOE. The tests included representative sets against Print, Scan, Copy, Fax send and Fax receive. Jobs were attempted to be submitted, viewed, modified, and deleted by the following user classes:

a. *The job owner (with the appropriate functional access);*
b. *The job owner (without the appropriate functional access);*
c. *An unknown (non-existing) user;*
d. *No userid specified;*
e. *U.ADMIN;*
f. *U.NORMAL; and*
g. *Unauthenticated.*

The test steps performed by the evaluator for this test activity are detailed throughout [ETProcRes] including section 4.2.6 and section 4.2.28. The actual results met the expected results.

2.3.4 FDP_DSK_EXT.1.1

2.3.4.1 Application Note:

If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The ST Author should consult with a CC Scheme for advice on approved Protection Profiles.

2.3.5 FDP_DSK_EXT.1.2

2.3.5.1 Application Note:

The intent of this requirement is to specify that encryption of any confidential data will not depend on a user electing to protect that data. The encryption specified in FDP_DSK_EXT.1 occurs transparently to the user and the decision to protect the data is outside the discretion of the user.

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.

2.3.5.2 TSS Activity:

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 Comment:

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.

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

2.3.5.3 Operational Guidance 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 Comment:

*Section **Configuring printer hard disk encryption** in the [EWS_Admin_Guide] and in the [CC_Supp] document describe the steps needed to enable the Device encryption function. There is only one hard disk drive in the TOE.*

2.3.5.4 KMD 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 Comment:

Section 2. Key Management Description in the [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.

2.3.5.5 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 User documents and Confidential TSF data.

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

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

Evaluator Comment:

The evaluator witnessed developer testing 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, held fax jobs). The developer then removed the hard disk from the TOE and analyzed it to ensure that none of the known data was present in plaintext. The developer then demonstrated that the data could be decrypted and made available.

The test steps performed for this test activity are detailed in [ETProcRes] section 4.2.7. The actual results met the expected results.

2.3.6 FDP_FXS_EXT.1

2.3.6.1 Application Note:

FDP_FXS.EXT.1 is required if fax-net separation is performed by the TSF.

Assurance Activity:

The following assurance activities are required when the TOE has a fax communication function to transmit and receive via PSTN.

2.3.6.2 TSS Activity:

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

1. The fax interface use cases
2. The capabilities of the fax modem and the supported fax protocols
3. The data that is allowed to be sent or received via the fax interface
4. How the TOE can only be used transmitting or receiving User Data using fax protocols

Evaluator Comment:

Section 7.1.8 of the [ST] describes basic fax interface use cases and the Fax-Network separation.

The fax modem supports only T.4 and T.30 protocols and disallows telnet, FTP and other protocols that could be used over an analog fax line.

The data that is allowed to be sent or received via the fax interface is noted in Section 7.1.2 under 'Fax Sending and Scan (Fax E-mail Server)' and 'Incoming Fax'.

Separation of the fax and other interfaces is described in Section 7.1.8 of the [ST].

2.3.6.3 Operational Guidance Activity:

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

Evaluator Comment:

*Section **Faxing** in the [CX725_CX727_User's_Guide] and in the [XC4100_User's_Guide] describes the fax interface in terms of usage and available features. Section **Configuring fax** in the [CC_Supp] discusses the configuration of the fax for the evaluated configuration.*

2.3.6.4 Test Activity:

The evaluator shall test to ensure that the fax interface can only be used transmitting or receiving User Data using fax protocols. Testing will be dependent upon how the TOE enforces this requirement. The following tests shall be used and supplemented with additional testing or a rationale as to why the following tests are sufficient:

1. Verify that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. For example, this may be achieved using a terminal application to issue modem commands directly to the TOE from a PC modem (issue terminal command: 'ATDT <TOE Fax Number>') – the TOE should answer the call and disconnect.
2. Verify TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. For example, this may be achieved by using a PC modem to attempt to receive a call from the TOE (submit a fax job from the TOE to <PC modem number>, at PC issue terminal command: 'ATA') – the TOE should disconnect without negotiating a carrier.

Evaluator Comment:

The evaluator performed tests to ensure that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. This was achieved by dialing the TOE from a Data Modem and witnessing the TOE answer the call and disconnect.

The evaluator performed tests to ensure that the TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. This was achieved by using a Data Modem to attempt to receive a call from the TOE. The TOE failed to negotiate a call using a data carrier.

The test steps performed by the evaluator for this test activity are detailed in [ETProcRes] section 4.2.28. The actual results met the expected results.

2.3.7 FDP_RIP.1(a) Subset Residual Information Protection

Assurance Activity:

2.3.7.1 TSS 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 Comment:

Section 7.1.9 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.

2.3.7.2 Operational Guidance Activity:

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

Evaluator Comment:

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

2.3.7.3 Test Activity:

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

Evaluator Comment:

The evaluator witnessed developer-performed testing 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] section 4.2.8. The actual results were the same as the expected results.

2.3.8 FDP_RIP.1(b) Subset Residual Information Protection

Assurance Activity:

2.3.8.1 TSS 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 Comment:

Section 7.1.9 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.

2.3.8.2 Operational Guidance Activity:

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

Evaluator Comment:

*Sections **Erasing printer memory** and **Erasing printer hard disk memory** in the [EWS_Admin_Guide] and in the [CX725_CX727_User's_Guide] and in the [XC4100_User's_Guide] have instructions for erasing printer nonvolatile memory and erasing the hard disk, respectively.*

2.3.8.3 Test Activity:

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

Evaluator Comment:

The evaluator witnessed developer-performed testing which caused the TOE to zeroize (purge) data on the Hard Disk and Flash storage. The evaluator examined the Hard Disk and Flash storage to confirm

that the purge data function had executed successfully. The test steps performed for this test are detailed in [ETProcRes] section 4.2.9.

2.4 Class FIA: Identification and Authentication

2.4.1 FIA_AFL.1 Authentication Failure Handling

2.4.1.1 Application Note:

This SFR applies only to internal identification and authentication.

Assurance Activity:

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

Evaluator Comment:

Section 7.1.1 of the [ST] describes the actions in case of authentication failure. The account is locked for an administrator configurable time period.

2.4.1.3 Operational Guidance 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 Comment:

*Section **Setting login restrictions** in the [EWS_Admin_Guide] and section **Configuring login restrictions** in the [CC_Supp] document discuss the settings Login failures 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.*

2.4.1.4 Test 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 Comment:

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] section 4.2.10. The actual results were the same as the expected results.

2.4.2 FIA_ATD.1 User Attribute Definition

2.4.2.1 Application Note:

The list of security attributes should be the union of all attributes for each of the supported authentication methods.

Assurance Activity:

2.4.2.2 TSS 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 Comment:

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

2.4.3 FIA_PMG_EXT.1 Extended: Password Management

2.4.3.1 Application Note:

This SFR applies only to password-based single-factor Internal Authentication.

Assurance Activity:

2.4.3.2 Operational Guidance 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 Comment:

*Section **Creating local accounts** in the [CC_Supp] 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*** *in the [CC_Supp] document has instructions for setting the minimum password length and recommends that passwords be at least 15 characters. The maximum password length is 32 characters.*

2.4.3.3 Test Activity:

The evaluator shall also 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 Comment:

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] section 4.2.11.

2.4.4 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

2.4.4.1 *Application Note:*

The TOE must support pre-shared keys for use in the IPsec protocol. There are two types of pre-shared keys--text-based (which are required) and bit-based (which are optional)--supported by the TOE, as specified in the requirements below. The first type is referred to as "text-based pre-shared keys", which refer to pre-shared keys that are entered by users as a string of characters from a standard character set, similar to a password. Such pre-shared keys must be conditioned so that the string of characters is transformed into a string of bits, which is then used as the key.

The second type is referred to as "bit-based pre-shared keys" (for lack of a standard term); this refers to keys that are either generated by the TSF on a command from the administrator, or input in "direct form" by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning" as was the case for text-based pre-shared keys. An example would be a string of hex digits that represent the bits that comprise the key.

The requirements below mandate that the TOE must support text-based pre- shared keys and optionally support bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done either by the TOE or in the Operational Environment.

2.4.5 FIA_PSK_EXT.1.3

2.4.5.1 Application Note:

For the length of the text-based pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.

In the second selection for FIA_PSK_EXT.1.3, the ST author fills in the method by which the text string entered by the administrator is "conditioned" into the bit string used as the key. This can be done by using one of the specified hash functions, or some other method through the assignment statement. If "bit-based pre-shared keys" is selected, the ST author specifies whether the TSF merely accepts bit based pre-shared keys, or is capable of generating them. If it generates them, the requirement specified that they must be generated using the RBG specified by the requirements. If the use of bit-based pre-shared keys is not supported, the ST author chooses "use no other pre-shared keys".

Assurance Activity:

2.4.5.2 Operational Guidance 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 Comment:

*Section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] document specifies that preshared keys must have at least 22 characters and be composed of a combination of uppercase and lowercase letters, numbers, and special characters. The allowable characters for pre-shared keys are any characters that can be entered through the printer's touch screen or keypad.*

2.4.5.3 TSS 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 pre- shared keys for each protocol identified in the requirement, or generating a bit- based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Evaluator Comment:

Section 7.1.4 of the [ST] describes the use of pre-shared keys. Pre-shared keys may be 1 to 36 characters in length, and are conditioned using SHA-1 or SHA-256. The conditioning is consistent with the selection in the requirement.

2.4.5.4 Test 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 Comment:

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] section 4.2.27. The actual results were the same as the expected results.

2.4.6 FIA_UAU.1 Timing of Authentication

2.4.6.1 Application Note:

User authentication may be performed internally by the TOE or externally by an External IT Entity.

Assurance Activity:

2.4.6.2 TSS 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 Comment:

Section 7.1.1 of the [ST] describes the authentication mechanisms provided for the evaluated configuration. These are: smart card authentication, username and password (internal) and username and password LDAP+GSSAPI.

Section 7.1.1 of the [ST] describes the interfaces used for authentication. For smart card authentication, it is the attached card reader and the touch panel. For the username and password authentication options, it 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]. Submission of network print jobs is permitted. Viewing of the operational status of the device is also described.

2.4.6.3 Operational Guidance 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 Comment:

*A description of LDAP or LDAP+GSSAPI authentication to the TOE is provided in section **Using LDAP or LDAP+GSSAPI** in the [EWS_Admin_Guide] and in section **Creating an LDAP or LDAP+GSSAPI login method** in the [CC_Supp] document. This is via a web interface.*

*A description of smartcard authentication to the TOE is provided in section **Configuring Smart Card Authentication Client** in the [CC_Supp] document or in section **Overview** in the [EWS_Admin_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 [EWS_Admin_Guide] and in section **Setting up local accounts** in the [CC_Supp] document.*

2.4.6.4 Test 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 the access to the TOE afterwards when using unauthorized data.

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

Evaluator Comment:

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 of the interfaces where applicable (embedded web server, touch screen). The test steps performed by the evaluator for this test are detailed in [ETProcRes] section 4.2.12. The actual results were the same as the expected results.

2.4.7 FIA_UAU.7 Protected Authentication Feedback

2.4.7.1 Application Note:

FIA_UAU.7 applies only to authentication processes in which the User interacts with the TOE.

Assurance Activity:

2.4.7.2 TSS 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 Comment:

Section 7.1.1 of the [ST] describes the authentication information feedback provided to users while authentication is in progress.

2.4.7.3 Test 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 Comment:

*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] section 4.2.12. The actual results are the same as the expected results.*

2.4.8 FIA_UID.1 Timing of Identification

2.4.8.1 Application Note:

User identification may be performed internally by the TOE or externally by an External IT Entity.

Assurance Activity:

It is covered by assurance activities for FIA_UAU.1.

2.4.9 FIA_USB.1 User-Subject Binding

Assurance Activity:

2.4.9.1 TSS 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 Comment:

Section 7.1.1 of the [ST] describes the rules for associating security attributes with users. This description is consistent with the SFR.

2.4.9.2 Test 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 Comment:

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] section 4.2.6 as well as throughout the [ETProcRes] document. The actual results met the expected results.

2.5 Class FMT: Security Management

2.5.1 FMT_MOF.1 Management of Security Functions Behavior

Assurance Activity:

2.5.1.1 TSS 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 with the definition of the SFR.

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

Evaluator Comment:

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 Operational Guidance 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 Comment:

*Sections **Setting up and using the home screen applications**, **E-mailing**, **Setting up the printer to fax**, **Securing the printer,** and **Upgrading and migrating** in the [CX725_CX727_User's_Guide] and in the [XC4100_User's_Guide], and the entire [EWS_Admin_Guide] and [CC_Supp] document describe the management functions of the TOE.*

2.5.1.3 Test 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 Comment:

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;*
f. *System or network time source; and*
g. *Device functions (e.g., fax).*

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] including section 4.2.13. The actual results met the expected results.

2.5.2 FMT_MSA.1 Management of Security Attributes

Assurance Activity:

2.5.2.1 TSS 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 Comment:

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 Operational Guidance Activity:

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

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

Evaluator Comment:

*Section **Configuring the printer** in the [CC_Supp] document has a configuration checklist for the timing of modifying security attributes for configuring the printer. The [EWS_Admin_Guide] has sections **Managing login methods**, **Managing certificates**, and **Managing other access functions** with information on security operations for security attributes and given roles to those security attributes, consistent with the definition of the SFR.*

2.5.2.3 Test 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 Comment:

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] section 4.2.14. The actual results met the expected results.

2.5.3 FMT_MSA.3 Static Attribute Initialization

2.5.3.1 Application Note:

FMT_MSA.3.2 applies only to security attributes whose default values can be overridden.

Assurance Activity:

2.5.3.2 TSS 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 Comment:

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].

2.5.3.3 Test Activity:

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

2.5.4 FMT_MTD.1 Management of TSF data

Assurance Activity:

2.5.4.1 Operational Guidance 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 Comment:

*Management operations are described in sections **Setting up and using the home screen applications**, **E-mailing**, **Setting up the printer to fax**, **Securing the printer**, and **Upgrading and migrating** in the [CX725_CX727_User's_Guide] and in the [XC4100_User's_Guide], and the entire [EWS_Admin_Guide] and [CC_Supp] document 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 **Editing or deleting local account groups** in the [EWS_Admin_Guide] and in the [CC_Supp] document discusses the editing or deleting of local account groups.*

*Section **Managing login methods** in the [EWS_Admin_Guide] and section **Configuring the printer** in the [CC_Supp] document discuss how security attributes are assigned and managed.*

*Section **Managing login methods** in the [EWS_Admin_Guide] and section **Configuring the printer** in the [CC_Supp] document describe how the security-related rules are configured.*

2.5.4.2 Test 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 Comment:

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 SFR 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.

The test steps performed by the evaluator occur across many tests documented in the [ETProcRes]. The actual results met the expected results.

2.5.5 FMT_SMF.1 Specification of Management Functions

2.5.5.1 Application Note:

Regarding "management functions provided by the TSF", the ST Author should consider management functions that support the security objectives of this protection profile.

The management functions should be restricted to the authorized identified role in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1.

The ST Author may identify cases where a security objective is fulfilled without explicit manageability.

For example, the following management functions are categorized by security objectives:

For O.USER_AUTHORIZATION, O.USER_I&A, O.ADMIN_ROLES, O.ACCESS_CONTROL:

- User management (e.g., add/change/remove local user)
- Role management (e.g., assign/deassign role relationship with user)
- Configuring identification and authentication (e.g., selecting between local and external I&A)
- Configuring authorization and access controls (e.g., access control lists for TOE resources)
- Configuring communication with External IT Entities

For O.UPDATE_VERIFICATION:

- Configuring software updates

For O.COMMS_PROTECTION:

- Configuring network communications
- Configuring the system or network time source

For O.AUDIT:

- Configuring data transmission to audit server
- Configuring the system or network time source
- Configuring internal audit log storage

For O.STORAGE_ENCRYPTION, O.KEY_MATERIAL:

- Configuring and invoking encryption of Field-Replaceable Nonvolatile Storage Devices

(Optional) For O.IMAGE_OVERWRITE, O.PURGE DATA:

- Configuring and/or invoking image overwrite functions
- Configuring and/or invoking data purging functions

Assurance Activity:

2.5.5.2 TSS Activity:

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

Evaluator Comment:

The management functions described in Table 22 (in the TSS) are consistent with those described in FMT_SMF.1. The table provides the permissions required by the U.ADMIN user in order to perform the listed functions.

2.5.5.3 Operational Guidance 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 Comment:

The management functions for the TOE are described in the documents [Menus_Guide], [EWS_Admin_Guide], and [CC_Supp]. 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

Assurance Activity:

2.5.6.1 TSS 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 Comment:

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 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 Comment:

In the tests performed for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1, the evaluator confirmed that the TSF maintains the roles U.ADMIN and U.NORMAL. The actual results met the expected results.

2.6 Class FPT: Protection of the TSF

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

Assurance Activity:

2.6.1.1 KMD 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 Comment:

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

The evaluator verified that section 2. Key Management Description in the [KMD] describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.

2.6.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data

2.6.2.1 Application Note:

The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through "normal" interfaces. While it is understood that the administrator could directly read memory to view these keys, doing so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not engage in such an activity.

Assurance Activity:

2.6.2.2 TSS 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 Comment:

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.

2.6.3 FPT_STM.1 Reliable Time Stamps

2.6.3.1 Application Note:

The time may be set by a trusted administrator or by a network service (e.g., NTP) from a trusted External IT Entity.

Assurance Activity:

2.6.3.2 TSS Activity:

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

Evaluator Comment:

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.

2.6.3.3 Operational Guidance Activity:

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

Evaluator Comment:

*Section **Setting the date and time** in the [EWS_Admin_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 [CC_Supp] 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**.*

2.6.3.4 Test 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 Comment:

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] section 4.2.16. The actual results met the expected results.

2.6.4 FPT_TST_EXT.1 Extended: TSF Testing

2.6.4.1 Application Note:

Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by verifying the TSF image by digital signature as specified in FCS_COP.1(b), or by hash specified in FCS_COP.1(c).

Assurance Activity:

2.6.4.2 TSS 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 Comment:

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. 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.

2.6.4.3 Operational Guidance 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 Comment:

Section Self-Test in the [SP] 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.

2.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

2.6.5.1 Application Note:

FPT_TUD_EXT.1.2 may be interpreted to allow an administrator to “pre-authorize” automatic updates, provided that they are verified according to FPT_TUD_EXT.1.3.

The digital signature mechanism is specified in FCS_COP.1(b). The published hash is generated by one of the functions specified in FCS_COP.1(c). It is acceptable to implement both mechanisms.

Assurance Activity:

2.6.5.2 TSS 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 Comment:

Section 7.1.7 of the [ST] describes firmware update. A digital signature on the firmware updated 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.

2.6.5.3 Operational Guidance 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 Comment:

*Section **Checking physical interfaces and installed firmware** in the [CC_Supp] document discusses how to obtain the firmware version.*

*Section **Updating firmware** in the [CC_Supp] document and in the [EWS_Admin_Guide] discusses how to start the firmware update.*

2.6.5.4 Test 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 Comment:

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] section 4.2.17. The actual results met the expected results.

2.7 Class FTA: TOE Access

2.7.1 FTA_SSL.3 TSF-Initiated Termination

Assurance Activity:

2.7.1.1 TSS 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 user inactivity.

Evaluator Comment:

Section 7.1.1 of the [ST] describes termination of user sessions for both the web interface and the touch panel, and specifies the administrator configurable period of inactivity range for each interface.

2.7.1.2 Operational Guidance 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 Comment:

*Section **Configuring login restrictions** in the [CC_Supp] 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 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 Comment:

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] section 4.2.18.

2.8 Class FTP: Trusted Paths/Channels

2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

2.8.1.1 Application Note:

The assignment in FTP_ITC.1.3 should address the confidentiality and/or integrity requirements for communication of User and TSF Data between the TOE and another IT entity. FTP_TRP.1 is intended to be used for interactive communication between the TOE and remote users.

The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. Protection (by one of the listed protocols) is required at least for communications with the server that collects the audit information. If it communicates with an authentication server (e.g., RADIUS), then the ST author chooses “authentication server” in FTP_ITC.1.1 and this connection must be protected by one of the listed protocols. If other authorized IT entities (e.g., NTP server) are protected, the ST author makes the appropriate assignments (for those entities) and selections (for the protocols that are used to protect those connections). After the ST author has made the selections, they are to select the detailed requirements in Appendix D.2 corresponding to their protocol selection to put in the ST. To summarize, the connection to an external audit collection server is required to be protected by one of the listed protocols. If an External Authentication server is supported, then it is required to protect that connection with one of the listed protocols. For any other external server, external communications are not required to be protected, but if protection is claimed, then it must be protected with one of the identified protocols.

While there are no requirements on the party initiating the communication, the ST author lists in the assignment for FTP_ITC.1.3 the services for which the TOE can initiate the communication with the authorized IT entity.

The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage. It may be the case that some part of the TOE setup involves manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to re- establish the communication automatically with (the necessary) manual intervention, there may be a window created where an attacker might be able to gain critical information or compromise a connection.

Assurance Activity:

2.8.1.2 TSS 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 Comment:

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.

*Section **Setting up Internet Protocol Security (IPSec)** in the [CC_Supp] document discusses the setup of IPSec communication between the printer and all network services including authentication, audit, e mail, and NTP. Section **Configuring IP Security (IPsec) settings** in the [EWS_Admin_Guide] also discusses the configuration of IPSec between the printer and the workstation or server.*

2.8.1.3 Test Activity:

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.
3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.
4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Further assurance activities are associated with the specific protocols.

Evaluator Comment:

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] section 4.2.19. The actual results met the expected results.

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

2.8.2.1 Application Note:

This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote administrators is performed over this path. The data passed in this trusted communication path are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Appendix D.2 corresponding to their selection are copied to the ST if not already present.

Assurance Activity:

2.8.2.2 TSS 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 Comment:

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.

2.8.2.3 Operational Guidance Activity:

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

Evaluator Comment:

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

2.8.2.4 Test Activity:

The evaluator shall also perform the following tests:

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

2. For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.
3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext.

Further assurance activities are associated with the specific protocols.

Evaluator Comment:

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 version 2.4.1) 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] section 4.2.20. The actual results met the expected results.

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

2.8.3.1 Application Note:

This requirement ensures that authorized remote users initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote users is performed over this path. The data passed in this trusted communication path are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures the detailed requirements in Appendix D.2 corresponding to their selection are copied to the ST if not already present.

Assurance Activity:

2.8.3.2 TSS 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 Comment:

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.

2.8.3.3 Operational Guidance Activity:

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

Evaluator Comment:

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

2.8.3.4 Test Activity:

The evaluator shall also perform the following tests:

1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote user access method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
2. For each method of remote access supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote user session without invoking the trusted path.
3. The evaluator shall ensure, for each method of remote user access, the channel data are not sent in plaintext.

Further assurance activities are associated with the specific protocols.

Evaluator Comment:

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 2.4.1) 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] section 4.2.21. The actual results met the expected results.

3 Security Assurance Requirements Activities

3.1 Class ASE: Security Target Evaluation

The ST is evaluated as per ASE activities defined 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.

Assurance Activity:

Evaluator Comment:

The quality of entropy in the random bit generator is discussed in the [EAR] document.

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 Comment:

A detailed description of the key management implementation, the Key Management Description, has been provided in the [KMD] document.

3.2 Class 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.

3.2.1 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.

3.2.1.1 Developer Note:

The developer shall provide appropriate TSS description and guidance documents as the functional specification. The TSS description identifies TSFIs associated with each SFR in order to confirm the validity of interface design. The developer is required to provide a description at least at a confirmable level in which TSS description and contents of guidance documents are consistent with each other. In case of insufficient information for evaluation in TSS description and contents of guidance documents, additional documentation can be requested. For the SFRs that cannot be directly operated/confirmed from external interfaces, the developer may be requested to provide additional information.

Assurance Activity:

3.2.1.2 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 Comment:

The identifiable external interfaces of power, touch screen or home screen, network, Graphical User Interface or Embedded Web Server, fax, and PKI card reader or smartcard reader are identified in the guidance documents of [CX725_CX727_User's_Guide] or [XC4100_User's_Guide], [Menus_Guide], [EWS_Admin_Guide], and [CC_Supp]. The TSS in section 7. TOE Summary Specification in the [ST] identifies all these interfaces required for realizing the SFRs. The description of the interfaces is consistent.

3.3 Class 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.

3.3.1 AGD_OPE.1 Operational User Guidance

3.3.1.1 Developer Note:

The developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Assurance Activity:

3.3.1.2 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 Comment:

*Section **Configuring the printer** in the [CC_Supp] document has a checklist of configuration items to confirm that the TOE returns to the evaluation configuration.*

3.3.1.3 Application Note:

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

3.3.2 AGD_PRE.1 Preparative Procedures

Assurance Activity:

3.3.2.1 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.

Assurance Activity:

Evaluator Comment:

The [CX725_CX727_User's_Guide] covers the CX725h printer claimed. The [XC4100_User's_Guide] covers the XC4150 printer claimed. These are both the printers identified in section 1.2 TOE Reference in the [ST].

*The [Menus_Guide], [EWS_Admin_Guide], and [CC_Supp] are generic guides. The specified supported printers in section **Overview and first steps** in the [CC_Supp] document include the CX725 with hard disk and XC4150 printers.*

3.4 Class ALC: Life-Cycle Support

At the assurance level provided for 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 evaluation at this assurance level.

3.4.1 ALC_CMC.1 Labelling of the TOE

Assurance Activity:

3.4.1.1 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 Comment:

Section 1.2 TOE Reference in the [ST] identifies the TOE as "Lexmark CX725h and XC4150 with firmware version CXTAT.040.204c3 with Lexmark Secure Element (P/N 57X0085)."

*Subsection **Supported printers** in the [CC_Supp] document lists the printers as the following:*

- *Lexmark CX725, with hard disk; and*
- *Lexmark XC4150, with hard disk.*

The [CX725_CX727_User's_Guide] specifies the CX725 printer. Document [XC4100_User's_Guide] covers the XC4150 printer. Both printers are shown on the Lexmark web site:
https://www.lexmark.com/en_CA/products/series/hardware-cx725-series.shtml or
https://www.lexmark.ddlbusiness.com/lexmark/lexmark-multifunction-printers/lexmark-xc4150/

3.4.2 ALC_CMS.1 TOE CM Coverage

Assurance Activity:

3.4.2.1 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 Comment:

Table 1 - CXTAT Evaluation Evidence References in section 2.2 Evaluation Evidence References in the [CL] document lists the evaluation evidence required by the SARs for this evaluation including the [ST], the [FSP], the [EAR], the [KMD], the [CC_Supp], the [Menus_Guide], [EWS_Admin_Guide], the [CX725_CX727_User's_Guide], and the [XC4100_User's_Guide].

3.5 Class ATE: Tests

3.5.1 ATE_IND.1 Independent Testing – Conformance

Assurance Activity:

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

The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each model either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

Evaluator Comment:

[ETProcRes] documents the testing aspects of the TOE. The table in section 4.2 Test Goal – Independent Evaluator Testing to the PP of the document shows the coverage of the Test assurance activities in the [PP_HCD].

The test plan covers the testing of the CX725h. This is identified in section 3.5.1 Equivalency Rationale in the [ETProcRes]. Both printer models have the exact same processor, ARMv8 1.2 Ghz processor, and firmware CXTAT.040.204c3. The differences in the two printers claimed in this evaluation are non-security relevant.

Setup needed beyond what is specified in the AGD documentation is discussed in section 3 Test Setup in the [ETProcRes] document.

The test objectives for the tests are discussed in section 4 Test Goals, Test Cases and Procedures in the [ETProcRes] document. The procedures include the goal of the procedure, the test steps executed, the expected results, and the actual results.

3.6 Class 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.

3.6.1 AVA_VAN.1 Vulnerability Survey

3.6.1.1 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 key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Evaluator Comment:

Section 4.3 Test Goal – Vulnerability Testing in the [ETProcRes] documents the vulnerability testing done by the evaluators which included a port scan of the CX725h in the evaluated configuration, scanning of the CX725h in the evaluated configuration with Nessus, an Internet search for vulnerabilities in the printers including the sources searched and the results obtained, and two vulnerability tests covering user data persistence and attempting to executed a faxed postscript file. No relevant vulnerabilities were found.