Lexmark MX931, MX951, MX953, CX730, CX930, CX950, CX951, CX952, CX953, CX931, CX961, CX962, CX963, and CX833 Multi-Function Printers with Hard Drive and without Fax, Firmware version 240.204CC

Security Target

Version 2.0

April 2026

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0	14 May 2025	Released for ATE submission.
1.1	21 May 2025	Update Common Criteria Installation Supplement and Administrator Guide version.
1.2	12 June 2025	Addressed Evaluator Ors
2.0	21 Apr 2026	Release for Assurance Maintenance

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Lexmark MX931, MX951, MX953, CX730, CX930, CX950, CX951, CX952, CX953, CX931, CX961, CX962, CX963, and CX833 Multi-Function Printers with Hard Drive and without Fax, Firmware version 240.204CC Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Lexmark MX931, MX951, MX953, CX730, CX930, CX950, CX951, CX952, CX953, CX931, CX961, CX962, CX963, and CX833 Multi-Function Printers with Hard Drive and without Fax, Firmware version 240.204CC
Security Target	Lexmark MX931, MX951, MX953, CX730, CX930, CX950, CX951, CX952, CX953, CX931, CX961, CX962, CX963, and CX833 Multi-Function Printers with Hard Drive and without Fax, Firmware version 240.204CC Security Target, v2.0

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) Collaborative Protection Profile for Hardcopy Devices, v1.0e (CPP_HCD_V1.0E)

1.4 Terminology

4 Terms used in this document are defined in Table 2 below and in Appendix G of the HCDcPP.

Table 2: Terminology

Term	Definition
AD	Active Directory
AES	Advanced Encryption Standard
BSD	Berkeley Software Distribution
CAVP	Cryptographic Algorithm Validation Program

Term	Definition
CBC	Cipher Block Chaining
CC	Common Criteria
CM	Configuration Management
CTR_DRBG	Counter Mode DRBG
DLE	Downloadable Emulators
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FAC	Function Access Control
FTP	File Transfer Protocol
GB	Gigabyte
GCM	Galois Counter Model
GSSAPI	Generic Security Services Application Program Interface
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
I&A	Identification & Authentication
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPP	Internet Printing Protocol
IPsec	Internet Protocol Security
ISO	International Standards Organization
IT	Information Technology
KAT	Known Answer Test
KDC	Key Distribution Center
KMD	Key Management Description

Term	Definition
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MFD	Multi-Function Device
MFP	Multi-Function Printer
NIAP	National Information Assurance Partnership
NAND	Not And
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PJL	Printer Job Language
PP	Protection Profile
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
RBG	Random Bit Generator
RFC	Request For Comments
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
ST	Security Target
TOE	Target of Evaluation
TPM	Trusted Platform Module
TRNG	True Random Number Generator

Term	Definition
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus

2 TOE Description

2.1 Deployment

5 The TOE is a digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents

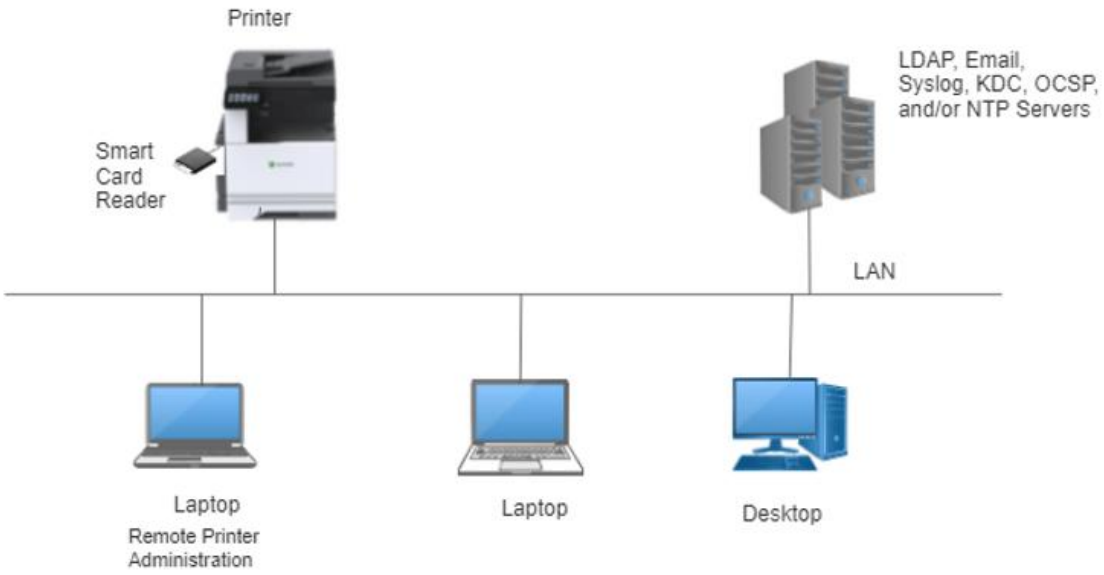

Figure 1: Example TOE deployment

2.2 Usage

6 The MFPs are multi-functional printer systems with scanning, and network capabilities. Their capabilities extend to walk-up scanning and copying; scanning to email; and servicing print jobs through the network. The MFPs feature an integrated touch-sensitive operator panel.

7 The major security features of the TOE are:

a) All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.

b) Administrators authorize Users to use the functions of the TOE.

c) User Document Data are protected from unauthorized disclosure or alteration.

d) TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.

e) TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.

f) Document processing and security-relevant system events are recorded, and such records are protected from disclosure to anyone except for authorized personnel. Records may not be altered.

8 The TOE includes a Trusted Platform Module (TPM), and a hard disk drive. The components that provide the TPM and hard drive can be standard or optional based on the TOE model.

9 The Lexmark printers are sold in predefined configurations, providing groupings of added options such as duplex printing, and hard drive. The configurations are identified by a character string appended to the model number. The following table provides details of the models and their configurations that are included in the evaluation.

2.3 Logical Scope

10 The TOE logical scope encompasses the following security functions:

a) **Identification, Authentication and Authorization.** When a touch panel or web session is initiated, the user is implicitly assumed to be the Guest (default) user. Per the evaluated configuration, the permissions for this user must be configured such that no access to TSF data or functions is allowed other than print job submission (job submission is authorized regardless of what user is logged in). Therefore, the user must successfully log in as a different user before any TSF data or functions other than print job submission may be accessed. TOE supports I&A with a per-user selection of Username/Password Accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment) using GSSAPI/Kerberos. Smart Card authentication may also be specified for users of the touch panel.

b) **Access Control.** Access controls configured for functions and menu access are enforced by the TOE.

c) **Encryption.** All user data submitted to the TOE and stored on the hard disk is encrypted to protect its confidentiality in the event the hard drive was to be removed from the MFP. The TOE protects the confidentiality and integrity of all information exchanged over the attached network by using IPSec with ESP for all network communication.

d) **Trusted Communication.** The TOE ensures communication is performed with known endpoints by using IPSec with pre-shared keys or by validating supplied certificates.

e) **Administrative Roles.** Through web browser and touch panel sessions, authorized administrators may configure access controls and perform other TOE management functions.

f) **Auditing.** The TOE generates audit event records for security-relevant events. Audit records are stored internally and securely transmitted to a remote IT system using the syslog protocol over IPsec.

g) **Trusted Operation.** Software updates are verified to ensure the authenticity of the software before being applied. During initial start-up, the TOE performs self-tests on its cryptographic components and the integrity of the executable code.

h) **Data Clearing and Purging.** In the evaluated configuration, the TOE automatically overwrites disk blocks used to store user data as soon as the data is no longer required.

2.4 Physical Scope

11 The physical boundary of the TOE is the software and hardware of the MFPs that include either standard or optional TPM and Hard disk components depending on the TOE model.

12 For some models, the TPM is an optional component that must be ordered and installed. This TPM optional component is referenced as Lexmark P/N 57x0195.

13 The TPM included in the printers is an Infineon OPTIGA™ Trusted Platform Module SLB9672_2.0 version 15.24.18954.00. The TPM provides a DRBG that is used to supply entropy to the Lexmark software DRBG.

14 The TPM implements a NIST SP 800-90A Revision 1 CTR_DRBG and has been evaluated and included on CMVP 4347 and the CAVP certificate A5852. Additionally, the TPM has been Common Criteria EAL4+ (AVA_VAN.4, ALC_FLR.1) certified (Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v15.24.18954.00).

15 The functionality of all models is the same; the differences are limited to color support, paper sizes supported, and pages per minute the printers support. The following table provides the printer specifics.

Table 3: TOE models

Build	Models included in the evaluation	Model Reference	Processor	TPM	HDD
MXTPM	MX931dse	MX931	Marvell 88PA6270 (G2)	Standard	P/N 27x0400
CXTMM	CX730de	CX730		Standard	P/N 27x0400
CXTPC	CX930dse	CX930		Standard	P/N 27x0400
	CX931dse	CX931		Standard	P/N 27x0400
	CX931dtse	CX931		Standard	P/N 27x0400
CXTLS	CX961se	CX961		Standard	P/N 27x0400
	CX961g	CX961		Standard	Standard
	CX961tse	CX961		Standard	P/N 27x0400
	CX961tg	CX961		Standard	Standard
	CX962se	CX962		Standard	P/N 27x0400
	CX962g	CX962		Standard	Standard
	CX962tse	CX962		Standard	P/N 27x0400
	CX962tg	CX962		Standard	Standard
	CX963se	CX963		Standard	P/N 27x0400

Build	Models included in the evaluation	Model Reference	Processor	TPM	HDD
	CX963g	CX963		Standard	Standard
	CX963xse	CX963		Standard	P/N 27x0400
	CX963xg	CX963		Standard	Standard
	CX833se	CX833		Standard	P/N 27x0400
	CX833g	CX833		Standard	Standard
	CX833xse	CX833		Standard	P/N 27x0400
	CX833xg	CX833		Standard	Standard
	CX950se	CX950		Standard	P/N 27x0400
	CX950g	CX950		Standard	Standard
	CX951se	CX951		Standard	P/N 27x0400
	CX951g	CX951		Standard	Standard
	CX952se	CX952		Standard	P/N 27x0400
	CX952g	CX952		Standard	Standard
	CX953se	CX953		Standard	P/N 27x0400
	CX953g	CX953		Standard	Standard
MXTLS	MX951se	MX951		Standard	P/N 27x0400
	MX951g	MX951		Standard	Standard
	MX953se	MX953		Standard	P/N 27x0400
	MX953g	MX953		Standard	Standard

Note: a=analog fax, d=duplex, e=e-task (touch screen device), f=staple finishing option, g=government, h=hard disk, m=mailbox, n=network, p=staple with hole punch finisher, s=stacker, t=additional tray included, v=vinyl, w=wireless, x=high-capacity feeder, z=VariTherm™ technology

16 Table 4 identifies the different Lexmark Family Group brand names for the TOE and equivalent Lexmark model. The differences between models and branding are not security relevant.

Table 4: TOE Branding Equivalency

Branding		Build
Sindoh	**Lexmark**	
CM2079	CX950g	CXTLS
CM3085	CX951g	
CM4095L	CX962g	
CM5105L	CX963g	
D500	CX950se	
D501	CX951se	
D750	CX962se	
D751	CX963se	
MF5103	MX953g	MXTLS
N720	MX953se	

17 The firmware version of the TOE is build 240.204CC, where build is as referenced in the table above. The first letter in the build identifier is M for mono printers or C for color printers. The next two letters are X for MFP and T for Touch. The last two letters signify the Model ID.

18 The hard disk component may be installed at the factory or by the customer. Installation depends on how the component is ordered (individually or as a predefined configuration). Installation instructions are included with the component if the customer is installing the components.

19 Lexmark uses reputable shipping firms that provide shipment tracking functionality to deliver printers and hard disks (ordered separately).

2.4.1 Guidance Documents

20 Lexmark provides the following product documentation in support of the installation and secure use of the TOE. The TOE guidance documentation shown below is available through the vendor's support portal and is available in .pdf and HTML format (Manuals and Guides (lexmark.com)). The Common Criteria Guide is provided by the vendor upon request.

a) Lexmark Common Criteria Installation Supplement and Administrator Guide, April 2026.

b) Lexmark MX931 MFP User's Guide, July 2024

c) Lexmark MX951 and MX953 MFP User's Guide, March 2026

d) Lexmark CX730, CX735, CX737, XC4342, XC4352 MFPs User's Guide, July 2024

e) Lexmark CX930, CX931, XC9325, XC9335 MFPs User's Guide, July 2024

f) Lexmark CX833, CX961, CX962, CX963, XC8355, XC9635, XC9645, XC9655 MFPs User's Guide, December 2024

g) Lexmark CX950, CX951, CX952, CX953, XC9525, XC9535 MFPs User's Guide, March 2026

h) Lexmark Embedded Web Server Administrator’s Guide, January 2023

2.4.2 Non-TOE Components

21 The TOE operates with the following components in the environment:

a) A LAN for network connectivity. The TOE supports IPv4 and IPv6.

b) An IT system acting as the remote syslog recipient of audit event records sent from the TOE.

c) IT systems that submit print jobs to the MFP via the network using standard print protocols.

d) An OCSP Server to verify the validity of X.509 certificates.

e) An IT system that connects remotely to the printer to perform remote configuration. Remote configuration is optional.

f) An LDAP Server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.

g) A card reader and cards to support Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card reader is the Identiv uTrust 2700 F Contact Smart Card Reader.

h) A Network Time Protocol Server. This system is optional based on if the time source is configured locally or remotely.

i) A Key Distribution Center (KDC). This system is optional and required only if smart card authentication is selected.

j) An email Server to receive outgoing emails from the printers. This system is optional and required only if email output is configured.

2.4.3 Functions not included in the TOE Evaluation

22 The following functionality is supported in the Lexmark printers but is not included in the evaluation:

a) In addition to Personal Identity Verification (PIV) cards, Common Access Card (CAC) and Secret Internet Protocol Router Network (SIPRNet) cards are also supported.

b) In addition to the Identiv uTrust 2700 F Contact Smart Card Reader, the following card readers are also supported:

Identiv uTrust 2700 R Contact Smart Card Reader,

Omnikey 3121 SmartCard Reader,

Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the Omnikey 3121 (example Omnikey 3021),

SCM SCR 331,

SCM SCR 3310v2.

c) Flash drive access is disabled to prevent flash drive print, scan and color printing jobs.

d) ThinPrint and AirPrint features are disabled.

e) Access to USB port is disabled.

f) Use of Wi-Fi interface is disabled.

2.4.4 CAVP Certificates

23 Users can verify the CAVP certificates by comparing the Lexmark module version listed in the certificate with the module version displayed when an administrator selects “device information” from the touch panel.

Table 5: CAVP certificates

Crypto Function	CAVP	Associated SFRs
AES (CBC)	#A6032, #A6033 (88PA6270 (G2)-64bit)	FCS_COP.1/DataEncryption FCS_COP.1/StorageEncryption FCS_IPSEC_EXT.1 FDP_DSK_EXT.1
DRBG (CTR_DRBG(AES))	#A6033 (88PA6270 (G2)-64bit)	FCS_CKM.1/SKG FCS_RBG_EXT.1
HMAC	#A6032, #A6033 (88PA6270 (G2)-64bit)	FCS_COP.1/KeyedHash FCS_IPSEC_EXT.1
RSA	#A6033 (88PA6270 (G2)-64bit)	FCS_CKM.1/AKG FCS_COP.1/SigGen
SHA	#A6032, #A6033 (88PA6270 (G2)-64bit)	FCS_COP.1/Hash FCS_IPSEC_EXT.1
CVL (IKEv1, IKEv2)	#A6033 (88PA6270 (G2)-64bit)	FCS_IPSEC_EXT.1
Finite field-based scheme	#A6033 (88PA6270 (G2)-64bit)	FCS_CKM.2

3 Security Problem Definition

24 The Security Problem Definition is reproduced from Appendix I of the HCDcPP.

3.1 Users

25 There are two categories of Users defined in this ST, Normal and Admin.

Table 6: User Categories

Designation	Name	Definition
U.NORMAL	Normal User	A User who has been identified and authenticated and does not have an administrative role
U.ADMIN	Administrator	A User who has been identified and authenticated and has an administrative role

26 A conforming TOE may allow additional roles, sub-roles, or groups. In particular, a conforming TOE may allow several administrative roles that have authority to administer different aspects of the TOE.

3.2 Assets

27 Assets are passive entities in the TOE that contain or receive information. In this PP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in this PP:

Table 7: Asset Categories

Designation	Asset category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

28 There are no additional Asset categories defined in this ST.

3.2.1 User Data

29 User Data are composed of two types:

Table 8: User Data Types

Designation	User Data type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form.
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job.

30 There are no additional types of User Data defined in this ST. Attributes associate documents and document processing jobs with the document processing functions of the TOE:

Table 9: Document and Job Attributes

Document processing function	Attribute
Printing	+PRT
Copying	+CPY
Scanning	+SCN

3.2.2 TSF Data

31 TSF Data are composed of two types:

Table 10: TSF Data Types

Designation	TSF Data type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable.
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE.

32 There are no additional TSF Data types defined in this ST.

3.3 Threats

33 The following threats are mitigated by this TOE:

Table 11: Threats

Identifier	Description
T.UNAUTHORIZED_ ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_FAILURE	A malfunction of the TSF may compromise the device security status if the TOE is permitted to operate.
T.UNAUTHORIZED_UP DATE	An attacker may install unauthorized firmware/software on the TOE to modify the Device security status.

Identifier	Description
T.NET_ COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.
T.WEAK_CRYPTO	An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes to access (read, modify, or delete) TSF and User data.

3.4 Assumptions

34 The following assumptions must be satisfied in order for the Security Objectives and Security Functional Requirements to be effective:

Table 12: Assumptions

Identifier	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

3.5 Organizational Security Policies

35 The following Organizational Security Policies (OSPs) are enforced by this TOE:

Table 13: Organizational Security Policies

Identifier	Description
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be stored within the TOE as well as protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices.

Identifier	Description
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.
P.WIPE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
P.ROT_INTEGRITY	The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.

4 Security Objectives

36 The following Security Objectives are satisfied by this TOE:

Table 14: Security Objectives for the TOE

Identifier	Description
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of firmware/software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTION	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.

Identifier	Description
O.AUDIT	The TOE shall generate audit data and store it internally as well as be capable of sending it to a trusted External IT Entity.
O.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data in Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.
O.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.
O.WIPE_DATA (optional)	The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
O.AUTH_FAILURES (conditionally mandatory)	The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
O.FW_INTEGRITY	The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.
O.STRONG_CRYPTO	The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

37 The following Security Objectives must be satisfied by the TOE's Operational Environment.

Table 15: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.

Identifier	Description
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

5 Security Requirements

5.1 Conventions

38 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

39 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the HCDcPP.

5.2 Extended Components Definition

40 The following list identifies the extended components used in this ST. All extended components are drawn from the HCDcPP.

- FAU_STG_EXT.1 Extended: External Audit Trail Storage
- FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
- FCS_IPSEC_EXT.1 Extended: IPsec selected
- FCS_KYC_EXT.1 Extended Key Chaining
- FCS_RBG_EXT.1 Extended: Random Bit Generation
- FDP_DSK_EXT.1 Extended: Protection of Data on Disk
- FDP_UDU_EXT.1 Extended: Document Unavailability
- FIA_PMG_EXT.1 Extended: Password Management
- FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FIA_X509_EXT.3 X.509 Certificate Requests
- FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
- FPT_SBT_EXT.1 Extended: Secure Boot
- FPT_SKP_EXT.1 Extended: Protection of TSF Data
- FPT_TST_EXT.1 Extended: TSF testing
- FPT_TUD_EXT.1 Extended: Trusted Update
- FPT_WIPE_EXT.1 Extended: Data Wiping

5.3 Functional Requirements

Table 16: Summary of SFRs

Class	SFRs
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_STG.1 Protected audit trail storage
	FAU_STG.4 Prevention of audit data loss
	FAU_STG_EXT.1 Extended: External Audit Trail Storage
Cryptographic Support (FCS)	FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)
	FCS_CKM.2 Cryptographic Key Establishment
	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
	FCS_IPSEC_EXT.1 Extended: IPsec selected
	FCS_KYC_EXT.1 Extended: Key Chaining
	FCS_RBG_EXT.1 Random Bit Generation
User Data Protection (FDP)	FDP_ACC.1 Subset access control

Class	SFRs
	FDP_ACF.1 Security attribute based access control
	FDP_DSK_EXT.1 Extended: Protection of Data on Disk
	FDP_UDU_EXT.1 Document Unavailability
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_PMG_EXT.1 Extended: Password Management
	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
	FIA_UAU.1 Timing of authentication
	FIA_UAU.7 Protected authentication feedback
	FIA_UID.1 Timing of identification
	FIA_USB.1 User-subject binding
	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication
	FIA_X509_EXT.3 X.509 Certificate Requests
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Privacy (FPR)	There are no class FPR requirements.
Protection of the TSF (FPT)	FPT_KYP_EXT.1 Extended: Protection of Key and Key Material
	FPT_SBT_EXT.1 Extended: Secure Boot
	FPT_SKP_EXT.1 Extended: Protection of TSF Data
	FPT_STM.1 Reliable time stamps

Class	SFRs
	FPT_TST_EXT.1 Extended: TSF testing
	FPT_TUD_EXT.1 Extended: Trusted Update
	FPT_WIPE_EXT.1/Disk Data Wiping
	FPT_WIPE_EXT.1/Flash Data Wiping
Resource Utilization (FRU)	There are no class FRU requirements.
TOE Access (FTA)	FTA_SSL.3 TSF-initiated termination
Trusted Paths/Channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel
	FTP_TRP.1/Admin Trusted path (for Administrators)
	FTP_TRP.1/NonAdmin Trusted path (for Non-Administrators)

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit;

c) All auditable events specified in Table 17, [*no other auditable events*].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 17**, [*no other audit relevant information*].

Table 17: Audit Events

Auditable Event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful login attempts limit is met or exceeded	FIA_AFL.1	None

Auditable Event	Relevant SFR	Additional information
Unsuccessful User authentication	FIA_UAU.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)
Unsuccessful User identification	FIA_UID.1	Supplied User ID/Name and origin of the attempt (e.g., IP address)
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1/Admin, FTP_TRP.1/NonAdmin	Reason for failure
Unsuccessful attempt to validate a certificate	FIA_X509_EXT.1	Reason for failure of certificate validation

FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*an Administrator*] with the capability to read [*all records*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG_EXT.1 Extended: External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 Refinement The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric keys)

FCS_CKM.1.1/AKG Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: **[**

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- FFC Schemes using ‘safe-prime’ groups that meet the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526].

].

FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric keys)

FCS_CKM.1.1/SKG Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1** and specified cryptographic key sizes [256 bits] that meet the following: [NIST SP 800-133 Rev.2 Section [6.1]].

FCS_CKM.2 Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- FFC Schemes using ‘safe-prime’ groups that meet the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526].

].

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

FCS_CKM.4 Cryptographic Key Destruction

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

- For volatile memory, the destruction shall be executed by a [removal of power to the memory];
- For non-volatile storage that consists of the invocation of an interface provided by the underlying platform that [
    - logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes, a new value of a key of the same size]];
    - instructs the underlying platform to destroy the abstraction that represents the key

] that meets the following: [*No Standard]*.

FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform **encryption/decryption** in accordance with specified cryptographic algorithms

- AES used in [CBC] mode,

  ] and cryptographic key sizes [

  Case: AES algorithm [

  [

    - [256 bits],

  ] that meet the following [

  Case: AES algorithm [
- ISO 18033-3, [CBC as specified in ISO 10116],

  ].

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash refinemenent The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [**SHA-256, SHA-384**] and message digest sizes [**selection: 256, 384]** that meet the following: **ISO/IEC 10118-3:2004**.

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-384], and cryptographic key sizes [256,384] and message digest sizes [256, 384] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation/Verification)

FCS_COP.1.1/SigGen The TSF shall perform [*cryptographic signature services (generation and verification*)] in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits, 3072 bits*]

that meets the following: [

Case: RSA schemes:

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5;ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3”

].

FCS_COP.1/StorageEncryption Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1/StorageEncryption The TSF shall perform [*data encryption/decryption*] in accordance with specified cryptographic algorithms

- AES used in [CBC] mode,

  ] and cryptographic key sizes [

  Case: AES algorithm [

  [

  - [256 bits],

  ] that meet the following [

  Case: AES algorithm [

- ISO 18033-3, [CBC as specified in ISO 10116],

  ].

FCS_IPSEC_EXT.1 Extended: IPsec selected

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

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-256 (RFC 3602)] together with a Secure Hash Algorithm (SHA)-based HMAC[HMAC-SHA-256, HMAC-SHA-384].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFCs 4109, [RFC 4304 for extended sequence numbers], and [no other RFC for hash functions]

IKEv2as defined in RFC 5996 and, [with no support for NAT traversal], and [no other RFCs for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms [AES-CBC-256 (specified in RFC 3602)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [

  length of time, where the time values can be configured within [*1-24*] hours;];
- IKEv2 SA lifetimes can be configured by a Security Administrator based on [

  length of time, where the time values can be configured within [*1-24*] hours]

  ].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [

  length of time, where the time values can be configured within [*1-8*] hours;];
- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [

  length of time, where the time values can be configured within [*1-8*] hours;]

  ].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*256*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1, IKEv2] exchanges of length [

according to the security strength associated with the negotiated Diffie-Hellman group;

at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups [

[14 (2048-bit MODP)], 15 (3072-bit MODP)] according to RFC 3526

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [SAN:IP address] and [no other reference identifier type].

FCS_KYC_EXT.1 Extended: Key Chaining

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [one] while maintaining an effective strength of [256 bits].

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

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR DRBG ([AES])].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one(1)*] hardware-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset access control

FDP_ACC.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in ~~**Table 4 and Table5**~~ Table 18 **and** Table 19**.**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in ~~**Table 4 and Table5**~~ Table 18 **and** Table 19**.**

FDP_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in ~~Table 4 and Table5~~** Table 18 **and** Table 19**.**

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

The Job Owner of submitted print jobs is determined by a Userid included in the embedded PJL. Print jobs received without a Userid, or with an unknown Userid, or with a Userid of a user that does not have the Held Jobs Access permission, are deleted after the specified timeout period for releasing held print jobs. During this time, no access to the print jobs is possible since access is restricted to the job owner

].

Table 18: D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	Operation:	Submit a document to be printed	View image or Release printed output	Modify stored document	Delete stored document
	Job owner (with Held Jobs Access)	Yes	Release	No	Yes
	Job owner (without Held Jobs Access)	Yes, but deleted	denied	denied	denied
	Unknown user	Yes, but deleted	denied	denied	denied
	No userid specified	Yes, but deleted	denied	denied	denied
	U.ADMIN	U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
	U.NORMAL	U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
	Unauthenticated	See above categories	denied	denied	denied
Scan	Operation:	Submit a document for scanning	View scanned image	Modify stored image	Delete stored image

		"Create"	"Read"	"Modify"	"Delete"
	Job owner (with E-mail Function permission)	Yes	No	No	No
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	Operation:	Submit a document for copying	View scanned image or Release printed copy output	Modify stored image	Delete stored image
	Job owner (with Copy Function permission)	Yes	No	No	Yes
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage/ Retrieval	Operation:	Store document	Retrieve stored document	Modify stored document	Delete stored document
	U.ADMIN	n/a	n/a	n/a	n/a
	U.NORMAL	n/a	n/a	n/a	n/a
	Unauthenticated	n/a	n/a	n/a	n/a

Table 19: D.USER.JOB Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	Operation:	Create print job	View print queue / log	Modify print job	Cancel print job
	Job owner (with Held Jobs Access)	Yes	Yes, for itself	Modify # of copies	Yes, for itself
	Job owner (without Held Jobs Access)	Yes, but deleted	denied	denied	denied

		"Create"	"Read"	"Modify"	"Delete"
	Unknown user	Yes, but deleted	denied	denied	denied
	No userid specified	Yes, but deleted	denied	denied	denied
	U.ADMIN	U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
	U.NORMAL	U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above.			
	Unauthenticated	See above categories	denied	denied	denied
Scan	Operation:	Create scan job	View scan status / log	Modify scan job	Cancel scan job
	Job owner (with E-mail Function permission)	Yes	No	No	No
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	Denied	Denied	Denied	Denied
Copy	Operation:	Create copy job	View copy status / log	Modify copy job	Cancel copy job
	Job owner (with Copy Function permission)	Yes	No	No	Yes
	U.ADMIN	denied	denied	denied	denied
	U.NORMAL	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage/ Retrieval	Operation:	Create storage / retrieval job	View storage / retrieval log	Modify storage / retrieval job	Cancel storage / retrieval job

		"Create"	"Read"	"Modify"	"Delete"
	Job owner	n/a	n/a	n/a	n/a
	U.ADMIN	n/a	n/a	n/a	n/a
	U.NORMAL	n/a	n/a	n/a	n/a
	Unauthenticated	n/a	n/a	n/a	n/a

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall [perform encryption in accordance with FCS_COP.1/StorageEncryption] such that any Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

FDP_UDU_EXT.1 Document Unavailability

FDP_UDU_EXT.1.1 The TSF shall ensure that any previous information content stored on a [non-wear-leveled storage device] of a resource is made unavailable [by overwriting data] upon the deallocation of the resource from the following objects: D.USER.DOC.

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*1 to 10*]] unsuccessful authentication attempts occur related to [

- *Local and remote login attempts*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the account for an administrator configurable amount of time*].

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Username, Password, Associated groups, User permissions as specified by associated groups, Time of the earliest authentication failure (since the last successful login if any have occurred), Number of consecutive authentication failures, Account lock status*].

FIA_PMG_EXT.1 Extended: Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters["!", "@", "#", "$", "%", "^", "&", "*", "(", ")", *[other ASCII characters except CR and NL]*];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [*lengths from 1 to 256 characters*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [*a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384*] and be able to [use no other pre-shared keys].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 Refinement: The TSF shall allow [*submit print jobs; view operational status of the device*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [*dots ("●")*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

FIA_UID.1.1 Refinement: The TSF shall allow [*submit print jobs, view operational status of the device*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*username, associated groups, User permissions*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [

- *The username are the values supplied by the user.*
- *The associated groups are the values configured for the user account.*
- *User permissions are determined by combining the configured permissions for each associated group.*

].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*the security attributes do not change during a session*].

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev Refinement: The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [IPsec] and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [accept the certificate].

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [

- *Audit*
- *Identification and authentication*
- *Authorization and access controls*
- *Communication with External IT Entities*
- *Network communications*
- *System or network time source*
- *Device functions*

] to [**U.ADMIN**].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 Refinement: The TSF shall enforce **the User Data Access Control SFP** to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*username, associated groups, user permissions]* to [*administrators authorized for access to the Security Menu*].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 Refinement: The TSF shall allow the [no role] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in ~~Table6~~** Table 20

Table 20: Management of TSF Data

Data	Operation	Authorized role(s)
TSF Data owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL		
User Job Data	Query, Modify	U.NORMAL
TSF Data not owned by a U.NORMAL		
Active Directory Configuration	Create	U.ADMIN
Date and Time Parameters	Query, Modify	U.ADMIN
Disk Encryption	Query, Modify	U.ADMIN
Enable Audit	Query, Modify	U.ADMIN
Enable HTTP Server	Query, Modify	U.ADMIN
Enable Remote Syslog	Query, Modify	U.ADMIN
Groups	Query, Modify, Delete, Create	U.ADMIN
Held Print Job Expiration Timer	Query, Modify	U.ADMIN
IPSec Settings	Query, Modify	U.ADMIN
Job Waiting	Query, Modify	U.ADMIN
Kerberos Setup	Query, Modify	U.ADMIN
LDAP Certificate Verification	Query, Modify	U.ADMIN
LDAP+GSSAPI – MFP Credentials	Query, Modify	U.ADMIN

Data	Operation	Authorized role(s)
LDAP+GSSAPI Configuration	Query, Modify, Delete, Create	U.ADMIN
Login Restrictions	Query, Modify	U.ADMIN
Network Port	Query, Modify	U.ADMIN
Permissions	Query, Modify	U.ADMIN
Remote Syslog Parameters	Query, Modify	U.ADMIN
Security Reset Jumper	Query, Modify	U.ADMIN
Smart Card Authentication Client Configuration	Query, Modify	U.ADMIN
SMTP Setup Settings	Query, Modify	U.ADMIN
SMTP Setup Settings - User-Initiated E-mail	Query, Modify	U.ADMIN
USB Buffer	Query, Modify	U.ADMIN
Username/Password Accounts	Query, Modify, Delete, Create	U.ADMIN
Visible Home Screen Icons	Query, Modify	U.ADMIN
Software, firmware, and related configuration data		
Firmware	Query	U.NORMAL
Firmware	Modify	U.ADMIN

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *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*
- *Configuring network communications*

- *Configuring the system or network time source*
- *Configuring data transmission to audit server*
- *Configuring internal audit log storage*
- *Configure applications*
- *Perform firmware updates*
- *Configure device functions*
- *Sanitize device.*

]

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [U.ADMIN, U.NORMAL].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.6 Protection of the TSF (FPT)

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [

- only store plaintext keys that meet any one of the following criteria [
  - The non-volatile memory the key is stored on is located in a protected storage device]].

FPT_SBT_EXT.1 Extended: Secure Boot

FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in a Root of Trust that is implemented in immutable code or a HW-based write-protection mechanism.

FPT_SBT_EXT.1.2 At boot time the TSF shall use the chain(s) of trust to confirm integrity of its firmware/software using a [hash, digital signature] verification method.

FPT_SBT_EXT.1.3 The TSF shall [halt boot process] in the event of a boot time verification failure so that the corrupted firmware/software isn't executed.

FPT_SBT_EXT.1.4 Following failure of verification, the TSF shall provide a mechanism to: [indicate a need to contact vendor support].

FPT_SBT_EXT.1.5 The TSF shall contain [hash data] in the Hardware Root of Trust.

FPT_SBT_EXT.1.6 The TSF shall make the symmetric key accessible only to the Hardware Root of Trust.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST_EXT.1 Extended: TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

FPT_TUD_EXT.1 Extended: Trusted update

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using [digital signature] and [no other functions] prior to installing those updates.

FPT_WIPE_EXT.1 Data Wiping

FPT_WIPE_EXT.1.1/Disk The TSF shall ensure that any previous customer-supplied information content of a resource in non-volatile storage is made unavailable upon the request of an Administrator to the following objects: [D.USER] using the following method(s): cryptographic erase and [

- logically addresses the storage location of the data and performs a [single] overwrite consisting of [zeroes]

] that meets the following: [no standard].

FPT_WIPE_EXT.1.1/Flash The TSF shall ensure that any previous customer-supplied information content of a resource in non-volatile storage is made unavailable upon the request of an Administrator to the following objects: [D.TSF] using the following method(s): cryptographic erase and [

- logically addresses the storage location of the data and performs a [single] overwrite consisting of [ones]

] that meets the following: [no standard].

5.3.7 TOE Access (FTA)

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate interactive session after a [*configurable time interval of user inactivity in the range of 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel*].

5.3.8 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall use **[IPsec] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: remote audit server, [authentication server, [*network time server and email server*]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

Application Note: Authentication server refers to both a KDC and a LDAP server (including Active Directory).

FTP_ITC.1.2 Refinement: The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for remote audit [*remote authentication, network time synchronization and sending email*].

FTP_TRP.1/Admin Trusted Path (for Administrators)

FTP_TRP.1.1/Admin Refinement: The TSF shall **use [IPsec] to** provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2/Admin Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin Refinement: The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

FTP_TRP.1/NonAdmin Trusted Path (for Non-administrators)

FTP_TRP.1.1/NonAdmin Refinement: The TSF shall **use [IPsec] to provide a trusted** communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*disclosure and detection of modification of the communicated data*].

FTP_TRP.1.2/NonAdmin Refinement: The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3/NonAdmin Refinement: The TSF shall require the use of the trusted path for [*initial user authentication and all remote user actions*].

5.4 Assurance Requirements

41 The TOE security assurance requirements are summarized in Table 21.

Table 21: TOE Security Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

6 TOE Summary Specification

6.1 Identification, Authentication and Authorization

SFRs: FCS_CKM_EXT.4, FIA_AFL.1, FIA_ATD.1, FIA_PMG_EXT.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FTA_SSL.3

42 Users are required to successfully complete the I&A process before they are permitted to access any restricted data or functionality. The set of restricted user functionality is under the control of the administrators, with the exception of submission of network print jobs which is always allowed.

43 A new session is established for the touch panel when the system boots and for web sessions when the connection is established. All sessions are initially bound to the Guest (default) user. In the evaluated configuration, the Guest user has no access to restricted functions or data other than allowing print jobs to be submitted.

44 Users must successfully authenticate to gain access to TOE functionality. Multiple login mechanisms are supported in the evaluated configuration: Smart Card authentication, Username/Password Accounts and LDAP+GSSAPI. Note that Smart Card and LDAP+GSSAPI authentications also use Kerberos functionality when authenticating certificates or credentials. Username/Password information is stored in flash.

45 For Smart Card authentication, no functions at the touch panel are allowed until I&A successfully completes. The touch panel displays a message directing the user to insert a card into the attached reader. Once a card is inserted, the user is prompted for a PIN. When the PIN is entered, only dots (“●”) are displayed. Once the PIN is collected (indicated by the user touching the Next button), the TOE passes the PIN to the card for validation. If it is not valid, a message is displayed on the touch panel and the user is asked to re-enter the PIN. After the card-configured number of consecutive invalid PINs, the card will lock itself until unlocked by a card administrator.

46 Upon successful card validation, the TOE forwards the certificate from the card to the configured Kerberos Key Distribution Center (KDC) (Windows Domain Controller) for validation. If the certificate validation is not successful, an error message is displayed on the touch panel until the current card is removed from the reader. If the certificate validation is successful, the TOE binds the username, account name, and email address (all obtained from the KDC/LDAP server) to the user session for future use. An audit record for the successful authentication is generated. All communication with the KDC and LDAP server uses IPsec.

47 For Username/Password Accounts and LDAP+GSSAPI, the TOE collects a username and password via the touch panel or via the browser session. On both interfaces, when the password is entered, only dots (“●”) are displayed. Once the username and password are collected, the next step in the process depends on the I&A mechanism being used.

48 For Username/Password Accounts, the TOE performs the validation of the username and password against the set of configured Username/Password Accounts. If the validation fails because of an invalid password (for a valid username), the count of failed authentication attempts is incremented for that account. If the threshold for failed attempts within a time period is reached, then the account is marked as being locked for the configured amount of time to mitigate against brute force password attacks.

49 For LDAP+GSSAPI, the TOE hashes the supplied password and forwards the username in an authentication request signed by the hashed password to the configured KDC for validation (using the configured machine credentials) and waits for the response. If no response is received, the validation is considered to have failed.

50 In the case of failed validations, an error message is displayed via the touch panel or browser session, and then the display returns to the previous screen for further user action. An audit record for the failed authentication attempt is generated.

51 If validation is successful, the TOE retrieves the account name and email address from the LDAP server and binds them to the user session for future use. An audit record for the successful authentication is generated.

52 Permissions for the user session are determined from group memberships. Authorized Administrators assign roles to user accounts by configuring permissions for each configured group and then assigning user accounts to groups. At minimum, during installation Authorized Administrators must perform the user account configuration activities in the guidance documentation to establish the evaluated configuration:

- Create new groups for Authorized Administrators and Authorized Users. The group names must correspond to names used in the LDAP server of Smart Card or LDAP+GSSAPI authentication is used.
- Configure appropriate permissions for each of those groups
- Assign all users and administrators using Username/Password Accounts to groups
- Modify the Public permissions (which are the only permissions for the Guest user account so that only B/W Print and Color Print are configured

53 For Username/Password accounts, the permissions for each group that the user is a member of (as specified in the account configuration) are combined. For Smart Cards and LDAP+GSSAPI, a list of group memberships are retrieved from the LDAP server. For each of those groups that match a group configured in the TOE, the permissions are combined. If the group memberships or permissions are changed, active sessions are not affected; the changes take effect at the next login.

54 The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for sessions expires. The timer values are separately configurable: 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel.

55 Users of the TOE, whether accessing the TOE via the touch panel or web interface, are considered to be in one or more of the following categories:

- Authorized Users – permitted to perform one or more of the user functions defined in FDP_ACC.1 and FDP_ACF.1.
- Authorized Administrators – permitted to access administrative functionality for control and monitoring of the MFP operation.
- Any Users – Authorized Users and Authorized Administrators

56 The following Permissions may be configured for groups:

Table 22: Management of TSF Data

Item	Description	Comment
Address Book	Controls the ability to manage the Address Book contents.	Permission may only be granted to authorized administrators in the evaluated configuration
Apps Configuration	Controls access to the configuration of any installed applications	Permission may only be granted to authorized administrators in the evaluated configuration.
B/W Print	Controls the ability to accept black and white print jobs.	Permission must be granted to the Public permissions
Cancel Jobs at the device	Controls access to the functionality to cancel jobs via the touch panel.	Permission may only be granted to authorized users in the evaluated configuration
Change Language from Home Screen	Controls access to the Change Language button on the Home screen (when displayed); this button is NOT displayed by default, but a user can activate it via the “General Settings Menu”	Permission may be granted to any users
Color Dropout	Controls a user’s ability to activate the Color Dropout functionality as part of a job; if protected and the user fails to authenticate, then the device DOES NOT use the color dropout functionality in the job	Permission may only be granted to authorized users in the evaluated configuration
Color Print	Controls the ability to print color jobs.	Permission must be granted to the Public permissions
Copy Color Printing	Controls a user’s ability to copy content in color	Permission may only be granted to authorized users in the evaluated configuration

Item	Description	Comment
Copy Function	Controls a user's access to the Copy functionality	Permission may only be granted to authorized users in the evaluated configuration
Create Profiles	Controls the ability to create scan profiles from remote systems.	Permission must not be specified for any user
Device Menu	Controls access to the Device administrative menu	Permission may only be granted to authorized administrators in the evaluated configuration
E-mail Function	Control's a user's access to the Email functionality (scan to email)	Permission may only be granted to authorized users in the evaluated configuration
Firmware Updates	Controls a user's ability to update the device's firmware code via the network	Permission may only be granted to authorized administrators in the evaluated configuration
Flash Drive Color Printing	Controls whether USB interfaces may be used for color print operations	Permission must not be specified for any user
Flash Drive Print	Controls whether USB interfaces may be used for black and white print operations	Permission must not be specified for any user
Flash Drive Scan	Controls whether USB interfaces may be used for scan operations	Permission must not be specified for any user
FTP Function	Controls a user's ability to access the FTP button on the Home Screen (when displayed).	Permission must not be specified for any user
Function Configuration Menus	Controls access to the configuration menus for the print, copy, e-mail and FTP functions.	Permission may only be granted to authorized administrators in the evaluated configuration
Held Jobs Access	Controls access to the Held Jobs function	Permission may only be granted to authorized users

Item	Description	Comment
		in the evaluated configuration
Import/Export Settings	Controls the ability to import and export configuration files	Permission may only be granted to authorized administrators in the evaluated configuration
Internet Printing Protocol (IPP)	Controls access to print job submission via IPP	Permission must not be specified for any user
Manage Bookmarks	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen	Permission must not be specified for any user
Manage Shortcuts	Controls access to the Manage Shortcuts Menu	Permission must not be specified for any user
Network/Ports Menu	Controls access to the Network/ Ports Menu	Permission may only be granted to authorized administrators in the evaluated configuration
New Apps	Controls access to configuration parameters for apps subsequently added to the device.	Permission may only be granted to authorized administrators in the evaluated configuration
Operator Panel Lock	Controls access to the “Lock Device” and “Unlock Device” buttons	Permission may only be granted to authorized users in the evaluated configuration
Option Card Menu	Controls a user’s ability to access the “Option Card Menu” that displays menu nodes associated with installed DLEs	Permission may only be granted to authorized administrators in the evaluated configuration
Out of Service Erase	Controls the ability to wipe the storage of the MFP when it is being taken out of service.	Permission may only be granted to authorized administrators in the evaluated configuration

Item	Description	Comment
Paper Menu	Controls access to the Paper Menu	Permission may be granted to any users
Remote Management	Controls whether or not management functions may be invoked from remote IT systems	Permission must not be specified for any user
Reports Menu	Controls access to the Reports Menu. This includes information about user jobs, which cannot be disclosed to non-administrators.	Permission may only be granted to authorized administrators in the evaluated configuration
Search Address Book	Controls access to the Search Address Book button that appears as part of the E-mail and FTP that are available from the panel's Home screen	Permission may be granted to any users
Security Menus	Controls access to the Security Menu	Permission may only be granted to authorized administrators in the evaluated configuration
Supplies Menus	Controls access to the Security Menu	Permission may only be granted to authorized administrators in the evaluated configuration
Use Profiles	Controls a user's ability to execute any profile	Permission must not be specified for any user

57 Consecutive login failures for each user account within a configured time period are tracked, and if the configured limit is reached the user account is automatically locked for the configured amount of time.

The TSF maintains the following security attributes for users:

- Username (configured for internal account, acquired from LDAP server AD and Smartcards)
- Password (internal accounts)
- Associated groups (configured for internal account, acquired from LDAP server AD and Smartcards)
- Permissions (dynamically determined by group memberships)
- Number of consecutive login failures
- Time of earliest login failure (since last successful login)

- Account lock status

58 Passwords for internal accounts are configured by administrators. The minimum password length is configurable from 1-32 characters. Passwords may contain any ASCII characters other than NL and CR. When Username/Password accounts are deleted, the associated password is destroyed in flash.

59 User interaction through the touch panel and web interface prior to successful authentication is limited to viewing the operational status of the device (e.g., low paper). Users may submit print jobs without authenticating, but the jobs are not printed until released by the authenticated user. When a password or PIN is entered for authentication, only dots ("●") are displayed.

60 User interaction through the touch panel and web interface prior to successful identification is limited to viewing the operational status of the device. Users may submit print jobs and supply identification via embedded PJL, but the jobs are not printed until released by the authenticated user. Invalid and missing identification in print jobs results in those print jobs being deleted.

61 Upon successful login, the username, associated groups and permissions are bound to the session. The username is the value specified during login or the username associated with the certificate from a smartcard. The groups are those configured internally or on the LDAP server. The permissions are the union of the permissions for each associated group. These bindings do not change during an active session. Upon expiration of an inactivity timer, the corresponding session is automatically terminated.

62 Communication with the Active Directory server uses IPsec. If Active Directory parameters are supplied and Join is selected, the parameter values are used to join the Active Directory Domain. If successful, machine credentials are generated and the LDAP+GSSAPI configuration parameters are automatically updated with the Domain and machine information.

63 Once the Domain has been joined, subsequent I&A attempts may use the LDAP+GSSAPI configuration to validate user credentials using the newly-created machine credentials as described above. The credentials specified for Active Directory by an authorized administrator are not saved.Access Control

SFRs: FDP_ACC.1, FDP_ACF.1

64 Access control validates a user access request against the session's permissions.

65 Authorization is restricted by not associating permission with a function.

66 When the FAC is a menu, access is also restricted to all submenus (a menu that is normally reached by navigating through the listed item). This is necessary for instances where a shortcut could bypass the listed menu. If a shortcut is used to access a sub-menu, the access control check for the applicable menu item is still performed (as if normal menu traversal was being performed).

67 When a function is restricted, the access control function determines if the user has permission to access the function. Normally the icons for the functions the user is not permitted to access are not displayed in the GUI.

68 The following table summarizes the access controls and configuration parameters used by the TOE to control user access to the MFP functions provided by the TOE. Additional details for each function are provided in subsequent sections.

Table 23: TOE user Function Access Control

Function	Access Control Rules	Configuration Parameter Rules
Print	Network print jobs can always be submitted. The job is held until released by a user who is authorized for the Held Jobs Access function and has the same userid as was specified in the SET USERNAME PJL statement. Network print jobs without a PJL SET USERNAME statement are automatically deleted after the expiry period for held jobs.	Allowed
Copy	Allowed if the user has permission to access Copy Function.	Allowed

6.1.1 Printing

69 Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded after the configured held jobs expiry period. Submitted jobs are always held In the TOE until released or deleted by a user authorized for the appropriate access control and who's userid matches the username specified when the job was submitted. Users are able to display the queue of their pending print jobs. If a held job is not released within the configured expiration time, the job is automatically deleted.

70 In the evaluated configuration, the setdevparams, setsysparams and setuserparams Postscript operators are made non-operational so that the Postscript DataStream cannot modify configuration settings in the TOE.

6.1.2 Copying

71 Copying is allowed if the user is authorized for the Copy Function access control.

6.2 Encryption

SFRs: FCS_CKM.1/SKG, FCS_CKM_EXT.4, FCS_CKM.4, FCS_COP.1/StorageEncryption, FCS_COP.1/DataEncryption, FCS_KYC_EXT.1, FCS_RBG_EXT.1, FDP_DSK_EXT.1, FPT_KYP_EXT.1

72 The following SFRs satisfy Encryption.

a) FCS_CKM.1/SKG An AES-256 key is generated for encryption of each of hard disk and flash configuration data.

b) FCS_CKM_EXT.4 The keys are destroyed when an administrator commands the decommission process to be performed.

c) FCS_CKM.4 Information regarding key destruction is provided in the KMD.

d) FCS_COP.1/StorageEncryption Document and configuration data is encrypted using AES-CBC-256.

e) FCS_COP.1/DataEncryption TSF configuration data in flash is encrypted using AES-CBC-256.

f) FCS_KYC_EXT.1 A key chain consisting of a single key is used. Details of the key chain are provided in the ancillary Key Management Description document. The key chain supports DEK outputs of no fewer than 256 bits.

g) FCS_RBG_EXT.1 An RBG function conforming to NIST SP 800-90A Revision 1 using CTR_DRBG(AES) is used to generate the 256-bit AES key for disk encryption. Entropy is provided by a hardware source that is described in more detail in the ancillary Entropy document.

h) FDP_DSK_EXT.1 All TSF is transparently encrypted in Flash. Flash encryption cannot be disabled. One Flash partition is dedicated to configuration data. The other Flash partitions are not encrypted.

i) FPT_KYP_EXT.1 Plaintext keys are not stored on the hard disk. Details of the key chain for the key are provided in the ancillary Key Management Description document.

73 All document data saved on the Hard Disk and configuration data in flash is encrypted using 256-bit AES. Encryption of the disk and flash is automatically enabled upon receipt of the printer from the factory. There is no administrator action required to enable printer encryption. Document data includes submitted print jobs, copy jobs waiting to be printed and scan jobs waiting to be emailed. The contents of each file are automatically encrypted (AES-CBC) as they are written to the Hard Disk and automatically decrypted when the contents are read. This security function is intended to protect against data disclosure if a malicious agent is able to gain physical possession of the Hard Disk. The entire disk drive is a single encrypted partition. Note that software is not stored on the drive and the drive is not the boot device. All TSF configuration data is automatically encrypted (AES-CBC) as it is written to flash and automatically decrypted when the contents are read.

74 A common key is used to encrypt all document data files, and a separate key is used to encrypt flash data. These keys are generated using the internal random number generator during initial installation of the HCD firmware. Details of the key chain for the key are provided in the ancillary Key Management Description document. The random number generator function conforms to NIST SP 800-90A Revision 1 using CTR_DRBG(AES) and is seeded with a minimum of 256 bits of entropy by a single hardware source described in the ancillary Entropy document.

75 The encryption keys are specific to the MFP. Any copy of the disk encryption key in RAM is destroyed when power is turned off.

6.3 Trusted Communications

SFRs: FCS_IPSEC_EXT.1, FIA_PSK_EXT.1, FCS_CKM.1/AKG , FTP_TRP.1, FCS_COP.1/KeyedHash, FIA_X509_EXT.1 X.509, FIA_X509_EXT.2 X.509

76 During TOE installation, a 3072-bit self-signed certificate for the device is generated in accordance with NIST SP 800-56B Revision 2 (“Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes).

77 IPSec with ESP operating in transport mode is required for all network datagram exchanges of any type with remote IT systems. This includes the following IT systems:

- Workstations submitting print jobs
- Workstations initiating connections to the web interface
- Remote Syslog server

- KDC
- LDAP server (including Active Directory)
- E-mail server
- OCSP server
- NTP

78 IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for IKE and ESP is AES-CBC-256. SHA-256 and SHA-384 are supported for HMACs. AES-CBC-256 may only be used if the IKE negotiation also selects AES-CBC-256.

79 ISAKMP and IKEv1/v2 are used to establish the Security Association (SA) and session keys for the IPSec exchanges. For IKEv1, Main Mode is always used for Phase 1 exchanges (Aggressive Mode is never used). No configuration is necessary. Diffie-Hellman is used for the IKE Key Derivation Function as specified in RFC2409, using Oakley Group 14 or Group 15. SA lifetimes for both IKEv1 and IKEv2 can be limited to separately configurable times for each phase: 1 to 24 hours for Phase 1, and 1 to 8 hours for Phase 2. IKEv1 complies with RFC2409 AND IKEv2 complies with RFC5996.

80 When the TOE receives an IKE proposal, it selects the first proposed DH group that matches a DH group configured in the TOE (DH Group 14 and Group 15 as specified in RFC 3526 Sections 3 and 4 are the only supported groups) and the negotiation will fail if there is no match. Similarly, when the TOE initiates the IKE protocol, a proposal is sent with all of the DH groups that are configured. The peer will select the first match from the IKE proposal against its configured DH groups; the negotiation fails if no match is found.

81 Peer authentication is performed using the RSA algorithm and certificates and/or pre-shared keys.

82 During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate or text-based Pre-Shared Keys (PSKs) may be configured by administrators and validated between endpoints. PSKs configured in the system may be 1 to 256 characters in length, composed of the characters specified in FIA_PSK_EXT.1.2, and are conditioned using a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384 according to RFC 2409 (for IKEv1) or RFC 5996 (for IKEv2). The key size specified in the SA exchange is 256 bits, the encryption algorithm is AES-CBC, and the Hash Authentication Algorithm is SHA-256, or SHA-384.

83 The secret value x used in the IKE key exchange using a 256-bit value obtained from the DRBG. Nonces used in IKE exchanges are generated using the random bit generator specified in FCS_RBG_EXT.1, with length at least equal to the security strength of the negotiated Diffie-Hellman group (112 bits for DH Group 14 (2048-bit MODP), 128 bits for DH Group 15 (3072-bit MODP)) and at least half the output size of the negotiated PRF hash (256 bits for HMAC-SHA2-256, 384 bits for HMAC-SHA2-384), with a minimum of 128 bits.

84 When certificates are used, the following certificate validation is performed:

85 The certificate path is validated, supporting a path length of 3. The signature in each certificate in the path, using 2048-bit or 3072-bit RSA digital signature algorithm, is verified using the public key of the issuing CA certificate in the device's trust store. The path must terminate with a CA certificate that has been configured as a trusted anchor.

86 All CA certificates in the path contain the basicConstraints extension with the CA flag set to TRUE. Certificate revocation status is checked using OCSP as specified in RFC 6960. If an OCSP Responder cannot be contacted, the certificate is accepted. Revocation checking is performed for the entire certificate chain for certificates received from IPsec peers and when certificates are imported.

87 In received certificates, the SAN: IP Address must be present and is used as the presented identifier. The certificate of the OCSP Responder must contain the OCSP Signing purpose. Validation of the Code Signing, Server Authentication and Client Authentication purposes is not performed by the TOE since TLS is not supported and code updates are not validated via certificates.

88 X.509 Certificate Signing Requests may be generated, containing Common Name, Organization, Organizational Unit, and Country values along with a generated 3072-bit RSA public key. Responses from a Certificate Authority are validated.

89 If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. The Security Policy Database is dynamically built with an accept/protect rule for each of the configured pre-shared keys and certificates, permitting packets from the addresses associated with them, and a default “final rule” to discard all other traffic. Incoming packets are validated against the SPD. Essentially incoming IP datagrams from authorized addresses (with PSKs or certificates) are accepted, and all other IP datagrams are discarded per the default final rule.

90 If external accounts are defined, LDAP+GSSAPI is used for the exchanges with the LDAP server. Kerberos v5 is supported for exchanges with the LDAP server.

91 All session keys are stored in dynamic RAM. Any copy of an RSA private key or PSK in RAM is destroyed when power is turned off.

92 The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 and HMAC-SHA-384, which operate on blocks of 512 and 1024 bits respectively, use key sizes of 256 and 384 bits respectively, and yield message digest sizes of 256 and 384 bits respectively.

93 A 3072-bit asymmetric key pair is generated in accordance with NIST SP 800-56B Revision 2 during installation. DH Group 14 and Group 15 are used in exchanges with peers to establish IPSec connections.

94 Session keys are destroyed when sessions terminate. PSKs are destroyed when the PSKs are deleted from the configuration by an authorized administrator. Session keys are destroyed when power is removed.

95 IPsec traffic is encrypted using AES-CBC-256. IPsec uses keyed-hash message authentication codes that are authenticated by the TOE.

96 X.509 certificates used in IPsec exchanges are validated. X.509 certificates may be used in IPsec exchanges for endpoint authentication. X.509 Certificate Signing Requests can be generated.

97 An RBG function conforming to NIST SP 800-90A Revision 1 using CTR_DRBG(AES) is used to generate the asymmetric key pair. Entropy is provided by a hardware source that is described in more detail in the ancillary Entropy document.

98 Text-based PSKs are supported and conditioned using a pseudo-random function (PRF) using HMAC-SHA2-256 or HMAC-SHA2-384 according to RFC 2409 (for IKEv1) or RFC 5996 (for IKEv2).

99 Trusted channels using IPsec are supported for authentication servers, remote audit servers, network time servers and email servers. Trusted paths using IPsec are

supported for administrators using the web interface. Trusted paths using IPsec are supported for users submitting print jobs.

6.4 Administrative Roles

SFRs: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MDT.1, FMT_SMF.1, FMT_SMR.1, FPT_SKP_EXT.1

100 The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. Authorization is granular, enabling different administrators to be granted access to different TSF data.

101 Authorized administrators (U.ADMIN) have one or more permissions to access management menus and/or functions (as defined in FMT_SMF.1). The following table provides a correlation between functions and the required permission.

Table 24: Function Correspondence to Permissions

Management Function	Required Permissions
User management	Security Menus
Role management	Security Menus
Configuring identification and authentication	Security Menus
Configuring authorization and access controls	Security Menus
Configuring communication with External IT Entities	Network/Ports Menu
Configuring network communications	Network/Ports Menu
Configuring the system or network time source	Network/Ports Menu
Configuring data transmission to audit server	Security Menus
Configuring internal audit log storage	Security Menus
Configure applications	Apps Configuration
Perform firmware updates	Firmware Updates
Configure device functions	Function Configuration Menus

Management Function	Required Permissions
Sanitize device	Out of Service Erase

102 If defined users have no management permissions, they are considered to have the U.NORMAL role and have no access to management functions or data. When new users are defined, by default they have no associated groups, and therefore no access to management functions or job functions (restrictive default attributes).

103 Neither the web interface nor the touch panel provide the ability to view the values of PSKs, symmetric keys or private keys for any administrator or user.

104 Administrators with the appropriate permissions have the ability to disable, enable and control the behavior of the specified functions.

105 Only administrators with the Security Menus permission may query, modify, delete or create user accounts or groups. By default, new users have no group memberships and therefore restrictive permissions. Administrators have one or more permission related to management functionality. Users have job function permissions only.

106 PSKs, symmetric keys and private keys are stored in flash. No mechanism is provided to read PSKs, symmetric keys or private keys.

6.5 Auditing

SFRs: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FAU_STG_EXT.1, FPT_STM.1

107 The TOE generates audit event records for security-relevant events. The events that cause audit records to be generated are specified in section Table 17. A time stamp is inserted into each record; reliable time is maintained via internal hardware or NTP. When NTP is used, it must be transmitted over IPsec (all communication with the TOE must use IPsec). A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated. Per the evaluated configuration, the severity level must be set to 5 (Notice).

108 Audit records are stored internally as well as being sent to a configured remote syslog server. Communication with the remote syslog server uses the Syslog protocol with IPsec.

109 Audit records for Successful Login events include the userid of the user as well as a session identifier. Other audit records include the session identifier, enabling the userid associated with other audit records to be determined via the corresponding Successful Login record. The time field in audit records is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured.

110 Audit records sent to the remote syslog server follow the syslog format defined in the Berkeley Software Distribution (BSD) Syslog Protocol (RFC 3164). The TOE supplies the PRI, HEADER, MSG/TAG, and MSG/CONTENT fields for all messages. The CONTENT portion may contain the following fields (in order, separated by commas):

- Event Number
- ISO 8601 time ([YYYY-MM-DD]T[hh:mm:ss])
- Severity

- Process (same as TAG)
- Remote IPv4 address
- Remote IPv6 address
- Remote Hostname
- Remote Port
- Local Port
- Authentication/Authorization method
- Username
- Setting ID
- Setting's old and new values
- Event name
- Event data

111 Fields in the CONTENT section that are not relevant for specific events are blank. The remote IPv4 address, remote IPv6 address, remote hostname, remote port, and local port fields are always blank for events resulting from actions at the MFP (e.g., usage of the touch panel).

112 Audit records are stored in the internal log as they are generated. If the internal audit log storage space usage reaches 98% of capacity, the oldest records are purged until used space is lowered to 80%.

113 Using the web interface, administrator with the Security Menu permission may upload the audit log in syslog or CSV format to their remote system via the browser connection. The audit log is saved as a local file and may be reviewed by the administrator. These administrators may also clear (empty) the audit log. When this action is performed, an Audit Log Cleared record is generated to note this action. Audit records may not be modified.

114 The TOE maintains a reliable time stamp via internal hardware or NTP. Audit records are stored in an internal log and transmitted to a remote syslog server. Storage space allocated for internal audit log storage is 1 MB. Users can be associated with audit events performed by identified users.

115 No users, or administrators without the Security Menu permission, may view, modify or delete audit records. Administrators with the Security Menu permission may view the internal audit log via the web interface. Only Administrators with the Security Menu permission may view the internal audit log. Only Administrators with the Security Menu permission may clear the internal audit log. No functionality is provided to modify audit records.

116 When the internal audit log space is exhausted, the oldest records in the log are discarded. Audit records are transmitted to a remote audit server via the syslog protocol over IPsec.

6.6 Trusted Operation

SFRs: FCS_COP.1/SigGen, FCS_COP.1/Hash, FPT_SBT_EXT.1, FPT_TST_EXT.1, FPT_TUD_EXT.1

117 During initial start-up, the TOE performs self-tests on the cryptographic components.

118 The following tests are performed during start-up:

- Executable code integrity testing – A digital signature (RSA 2048, SHA256) of the executable code is calculated and compared to a saved value in flash.
- Cryptographic algorithm testing – Uses Known Answer Tests (KATs) to verify proper operation of cryptographic functions.

119 During the boot cycle, the integrity of the executable code is validated. During manufacturing, write-once fuses are programmed with a hash of Lexmark's public code signing key. The boot ROM will refuse to load any code that is not signed by the key whose hash does not match that which was programmed at manufacturing.

120 At power on, the boot ROM looks for an image description table on the designated boot device. The image description table contains the size, location, and hash of the next stage boot loader (g2-loader), and a public key. The image description table is signed, and the boot ROM verifies the signature using the provided public key. The boot ROM also verifies that a hash of the public key matches the hash programmed in fuses. The boot ROM loads g2-loader into SRAM, verifies its hash, and control is passed to g2-loader.

121 g2-loader initializes DRAM and some other platform-specific pieces before loading the next stage boot loader, u-boot. g2-loader uses the same image description table for loading and verifying u-boot, and control is passed to u-boot.

122 u-boot then looks for a kernel (and optionally initramfs) to load. The entire cramfs partition is loaded into memory. At the end of the partition is a certificate with signature. u-boot verifies the signature of the entire partition, and verifies that the signature was made by the same key that is baked into u-boot (the public side of the key is hard-coded in u-boot source code). Control is passed on to the kernel in the boot partition.

123 The boot partition also contains information that is used by the dm-verity subsystem of the Linux kernel. This information is covered by the same signature as the rest of the boot partition. The kernel uses this information to create a dm-verity device, which the kernel then mounts for the root filesystem. Since changing any part of the root filesystem would invalidate the verity hashes, a read-only filesystem is required, for which Lexmark uses squashfs.

124 If code verification fails, all the imaging and mechanism control blocks of the HCD, as well as network and PCIe functionality, is disabled and the system halts. The only way to proceed is to reboot the HCD. The lack of the normal display on the HCD at boot completion indicates that vendor support should be contacted.

125 Other code partitions may be mounted by Linux at run-time, in which case a dm-verity device is created and mounted to ensure that the code is trusted.

126 Any writable filesystems are mounted as noexec so as to avoid inadvertently executing code from them, since any code stored there would not be covered by a trusted signature.

127 Lexmark uses full partition images for code update. That is, the code update file contains the entire partition for the new version of code, as opposed to doing per-file updates or delta-images. When a code update file is received by the device, it is saved to a writable filesystem, and then the device is rebooted into recovery mode (i.e., using the recovery boot and recovery root partitions). This avoids the complexity of rewriting a partition while concurrently running from it.

128 The code update information is validated in the same manner as described above for operational code – the code must be signed with a public key whose hash matches the value burned into fuses during manufacturing.

129 During operation, a SHA256 hash is maintained for each executable page. Before any page is loaded into memory, the hash is verified to ensure the code has not been modified since boot.

130 Administrators may use the web interface to query the current firmware version or supply firmware updates. Firmware updates must be digitally signed, and the TOE verifies the signature before applying the update.

131 Digital signatures of update files are authenticated before being applied. Digital signatures verification relies on hash algorithms supplied by the TOE.

132 On each boot, a hardware-based chain of trust is used to validate the integrity of the executable code. A set of self-tests are executed at start-up to verify correct operation of the TOE.

133 Administrators may use the web interface to query the current firmware version and supply signed updates.

6.7 Data Clearing and Purging

SFRs: FDP_UDU_EXT.1, FPT_WIPE_EXT.1/Disk, FPT_WIPE_EXT.1/Flash

134 D.USER.DOC is not stored on a wear-leveled device. Once a job has been completed, the document file on the hard disk (non-wear-leveled) is logically deleted and marked as needing to be overwritten. Until the overwriting occurs, the disk blocks containing the files are not available for use by any user. Every 5 seconds, the TOE checks to see if any “deleted” files are present and begins the disk overwriting process.

135 The TOE overwrites each block associated with each deleted file (including bad and remapped sectors) three times: first with “0x0F” (i.e., 0000 1111), then with “0xF0” (i.e., 1111 0000), and finally with a block of random data (supplied by the internal random number generator). Each time that the device overwrites a different file, it selects a different block of random data.

136 Once the disk overwriting is complete, the disk blocks used for the deleted files are once again available for use by the system. If the disk overwriting process is interrupted by a power cycle or reset, the status is remembered across the restart and the process resumes when operation resumes.

137 If any error occurs during the disk overwriting process, an audit record is generated, and the file system is considered to be corrupt and must be re-initialized.

138 The TOE also overwrites RAM with zeroes upon deallocation of any buffer used to hold user data.

139 Document data is overwritten when the file or memory containing the data is released.

140 An administrator may command the TOE to be sanitized (e.g., prepared for decommissioning). For this operation, the hard disk is zeroized, and all flash configuration data is overwritten with ones (flash is a wear-leveled device). In addition, the keys for the hard disk and flash configuration data are overwritten with zeroes. This wipes all D.USER from the hard disk (which contains no D.TSF) and D.TSF from flash storage (which contains no D.USER).

141 When purging is commanded by an administrator, the disk storage is zeroized. When purging is commanded by an administrator, flash storage is overwritten with ones.

6.8 Common Functionality regarding Key Destruction in Flash Memory

142 Multiple types of keys are stored in flash memory: RSA private keys and PSKs. The flash component performs wear leveling/garbage collection; therefore, physical copies of these keys may continue to exist inside the flash component for some period of time after they have been “overwritten” by the software.

143 The keys stored in flash are the RSA private keys associated with the device certs and the IPSec PSKs. When a single PSK is modified from the configuration by an administrator, the new value of the same size overwrites the old value. When an administrator requests the TOE to be sanitized (e.g., decommissioning), the location in flash holding the PSKs are overwritten once with ones. Therefore, the visible storage locations for these items from the flash component reflect the overwrites.

144 The disk encryption key (DEK) and the flash encryption key are stored in the TPM. These keys are cleared when the administrator requests the TOE to be sanitized. When this occurs, the Erase Printer Memory function is invoked. This function invokes the TMP2_Clear command which overwrites both keys with zeroes (instructs the underlying platform to destroy the abstraction that represents the key).

145 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.

7 Rationale

7.1 Conformance Claim Rationale

146 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is hardcopy device, consistent with the HCDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the HCDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the HCDcPP.

d) **Security requirements.** As shown in section 5 the security requirements are reproduced directly from the HCDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

147 The following table maps threats, OSPs, and assumptions, to their respective Security Objectives.

Table 25: Security Objectives Rationale

Threat/Policy/Assumptions	Rationale
T.UNAUTHORIZED_ACCESS An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component..	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_COMPROMISE An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component..	O.ACCESS_ CONTROL restricts access to TSF Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.
T.UNAUTHORIZED_UPDATE An attacker may cause the installation of unauthorized firmware/software on the TOE.	O.UPDATE_VERIFICATION verifies the authenticity of software updates.

Threat/Policy/Assumptions	Rationale
T.NET_COMPROMISE An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.	O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.
T.WEAK_CRYPTO An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes.	O.STRONG_CRYPTO implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy.
P.AUTHORIZATION Users must be authorized before performing Document Processing and administrative functions.	O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION The TOE must be able to identify itself to other devices on the LAN.	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices.	O.STORAGE_ENCRYPTION ensure User Document Data or Confidential TSF Data is encrypted and stored in Nonvolatile Storage devices.
P.KEY_MATERIAL Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.	O.KEY_MATERIAL protects from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices.
P.IMAGE_OVERWRITE (optional)	O.IMAGE_OVERWRITE (optional) ensures Upon completion or cancellation of a Document

Threat/Policy/Assumptions	Rationale
Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.	Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.
P.WIPE_DATA (optional) The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.	O.WIPE_DATA (optional) provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
P.ROT_INTEGRITY The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.	O.FW_INTEGRITY ensures TOE's own integrity has remained intact and attests its integrity to outside parties on request.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.	OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.
A.NETWORK The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.	OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.
A.TRUSTED_ADMIN TOE Administrators are trusted to administer the TOE according to site security policies.	OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.TRAINED_USERS Authorized Users are trained to use the TOE according to site security policies.	OE.USER_TRAINING ensures that Users are aware of site security policies and have the competence to follow them.

7.3 Security Assurance Requirements rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the cPP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.