Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e Multifunction Printer (MFP) Security Target
August 31, 2007
Document No. SV-0606-002(1.11)

Lexmark International, Inc.
740 New Circle Road NW
Lexington, KY 40550

Document Introduction

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Lexmark X646dte, X646e, X646ef, X850e, X852e, X854e, X940e and X945e Multifunction Printers (MFPs). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

List of Acronyms

CC ..... Common Criteria
EAL2 ..... Evaluation Assurance Level 2
IT ..... Information Technology
MFP ..... Multifunction Printer
NIAP ..... National Information Assurance Partnership
PP ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SFR ..... Security Functional Requirement
SOF ..... Strength of Function
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TSF Scope of Control
TSF ..... TOE Security Functions
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e Multifunction Printers (MFPs). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all international interpretations through September 28, 2006. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e Multifunction Printers (MFPs) Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e Multifunction Printers (MFPs) Security Target

1.1.2 Security Target Author

COACT, Inc.

1.1.3 Security Target Publication Date

August 31, 2007

1.1.4 TOE Reference

Lexmark X646dte (firmware revision LC2.MC.P239b), X646e (firmware revision LC2.MC.P239b), X646ef (firmware revision LC2.TI.P239b), X772e (firmware revision LC2.TR.P275), X850e (firmware revision LC2.BE.P238b), X852e (firmware revision LC2.BE.P238b), X854e (firmware revision LC2.BE.P238b), X940e (firmware revision LC.BR.P060) and X945e (firmware revision LC.BR.P060) Multifunction Printers (MFPs). Hereafter this document omits the references to the firmware revisions when referencing the MFP models.

1.1.5 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.1.6 Keywords

Multifunction Printer (MFP), Common Criteria (CC), User Authentication, Fax Communications Control, Device Configuration Protection, Evaluation Assurance Level 2 (EAL2), Security Target (ST), Security Function (SF), Security Function Policy (SFP), Target of Evaluation (TOE), TOE Security Functions (TSF), TOE Security Policy (TSP).

1.2 TOE Overview

This Security Target defines the requirements for the Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e MFPs Target of Evaluation (TOE).

The TOE is the complete MFP and implements the TOE Security Functions of Fax Communications Control, User Authentication, Device Configuration Protection, Hard Disk Encryption, and Hard Disk Sanitization.

A summary of the TOE security functions can be found in Section 2, TOE Description. A description of the security functions can be found in Section 6, TOE Summary Specification.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description and rationale of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 typically identifies any claims of conformance to a registered Protection Profile (PP). This Security Target, however, does not claim conformance to any registered Protection Profile.

Chapter 8 references the rationale for the security objectives, requirements, TOE Summary Specification and PP claims.

1.3 Common Criteria Conformance

The Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e Multifunction Printers (MFPs) is compliant with the *Common Criteria (CC) for Information Technology Security Evaluation, Version 2.3*, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL2.

1.4 Protection Profile Conformance

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 2

2. TOE Description

This chapter provides the context for the TOE evaluation by providing the following elements:

A) Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e MFP Product Description

B) MFP Architecture

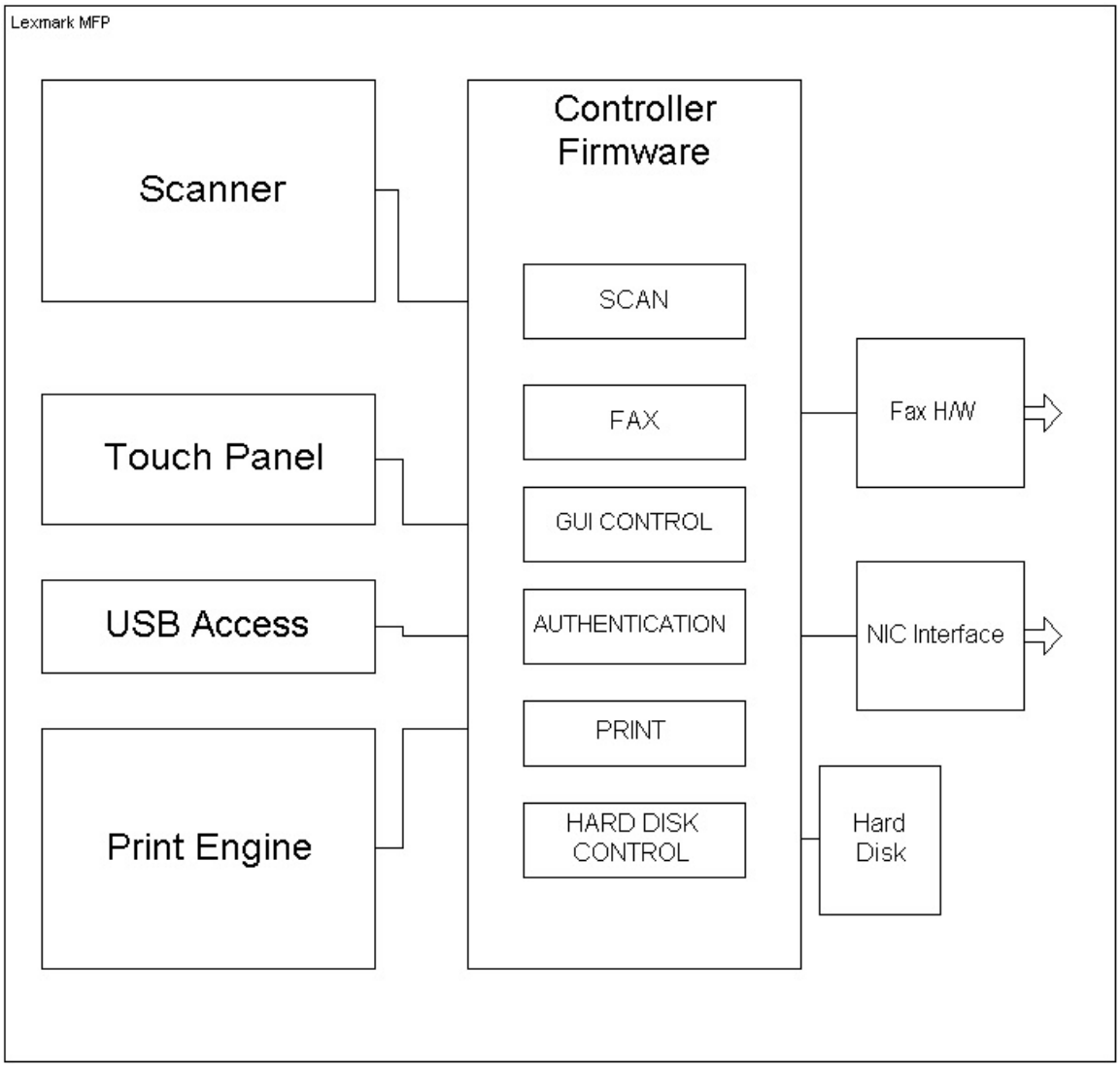
C) TOE Description, including a Description of the Physical and Logical TOE Boundaries

D) TOE Evaluated Configuration

2.1 Lexmark MFP Product Description

The Lexmark MFP, as shown in Figure 1, is a multi-functional printer system with scanning, fax, and networked capabilities. Its capabilities extend to walk-up scanning and copying, scanning to fax, scanning to email, and servicing print jobs through the network. The MFP also enables users to insert a USB Drive, which can be used as the source for print operations or the destination for scan operations. The MFP includes print, fax and scan functionality with an integrated touch-sensitive operator panel.

Figure 1. Lexmark MFP Product Description



The Lexmark MFP family included within this TOE includes an array of products that share a common set of functionality. Each of the MFPs included in the TOE includes a Hard Disk Drive (HDD) and security relevant functions relevant to the HDD. The following products share the security functions described in this document: the Lexmark X646dte MFP, X646e MFP, X646ef MFP, X772e MFP, X850e MFP, X852e MFP, X854e MFP, X940e MFP and X945e MFP. The differences between these products are not security relevant and are summarized in the following table.

Table 1 - Comparison of MFP Models and Nomenclature

MFP Model	Functionality
X646dte	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 48 ppm Print Speed (A4, Black) Duplex: Up to 36 spm Print Speed (Letter, Black): Up to 50 ppm

MFP Model	Functionality
	Print Speed (Letter, Black) Duplex: Up to 37 spm Time to First Page (Black) as fast as 8.5 seconds Copy Speed (Letter, Black): Up to 50 cpm
X646e	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 48 ppm Print Speed (Letter, Black): Up to 50 ppm Time to First Page (Black) as fast as 8.5 seconds Copy Speed (Letter, Black): Up to 50 cpm
X646ef	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 48 ppm Print Speed (A4, Black) Duplex: Up to 36 spm Print Speed (Letter, Black): Up to 50 ppm Print Speed (Letter, Black) Duplex: Up to 37 spm Time to First Page (Black) as fast as 8.5 seconds Copy Speed (Letter, Black): Up to 50 cpm
X772e	Print Technology Color Laser Print Speed (A4, Black): Up to 25 ppm Print Speed (A4, Black) Duplex: Up to < 13 spm Copy Speed (Letter, Black): Up to 24 cpm
X850e	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 35 ppm Print Speed (A4, Black) Duplex: Up to 35 spm Print Speed (Letter, Black): Up to 35 ppm Print Speed (Letter, Black) Duplex: Up to 35 spm Time to First Page (Black) as fast as 6.8 seconds Copy Speed (Letter, Black): Up to 35 cpm
X852e	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 45 ppm Print Speed (A4, Black) Duplex: Up to 45 spm Print Speed (Letter, Black): Up to 45 ppm Print Speed (Letter, Black) Duplex: Up to 45 spm Time to First Page (Black) as fast as 6.8 seconds Copy Speed (Letter, Black): Up to 45 cpm
X854e	Print Technology Monochrome Laser Print Speed (A4, Black): Up to 55 ppm Print Speed (A4, Black) Duplex: Up to 50 spm Print Speed (Letter, Black): Up to 55 ppm Print Speed (Letter, Black) Duplex: Up to 50 spm Time to First Page (Black) as fast as 6.8 seconds Copy Speed (Letter, Black): Up to 55 cpm
X940e	Print Technology Color Laser Print Speed (A4, Black): Up to 40 ppm Print Speed (A4, Black) Duplex: Up to 37 spm Copy Speed (Letter, Black): Up to 40 cpm
X945e	Print Technology Color Laser Print Speed (A4, Black): Up to 45 ppm Print Speed (A4, Black) Duplex: Up to 37 spm Copy Speed (Letter, Black): Up to 45 cpm

2.2 TOE Description

This Security Target defines the requirements for the Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e MFPs Target of Evaluation (TOE).

The TOE is the complete MFP and implements the TOE Security Functions of Fax Communications Control, User Authentication, Device Configuration Protection, Hard Disk Encryption, and Hard Disk Sanitization.

2.3 TOE Physical Boundary

This section provides context for the TOE evaluation by describing the physical boundary of the TOE. The physical boundary of the TOE consists of the all of the MFP hardware and firmware.

2.4 Logical Boundary

The logical TOE boundaries are defined by the TOE security functions as described in the following sections.

2.4.1 Fax Communications Control

The Fax Communications Control security function assures that the information on the TOE, and the information on the network to which the TOE is attached, is not exposed through the phone line that provides connectivity for the analog fax function. This function assures that only printable documents are accepted via incoming fax connections, and that the only thing transmitted over an outgoing fax connection is the document that was submitted for faxing.

The Fax Communications Control security function is inherent in the design of the system, and is not explicitly activated. Control of the fax functionality is incorporated directly into the TOE's firmware. The fax chip that sends and receives data over the phone line is directly controlled by the TOE firmware. The modem chip is in a mode that's more restrictive than Class 1 mode, and relies on the TOE firmware for composition and transmission of fax data. The TOE firmware explicitly disallows the transmission of frames in data mode and allows for the sending and receiving of facsimile jobs, only. There is no mechanism by which telnet, FTP, or other network protocols can be sent or received over the analog fax line.

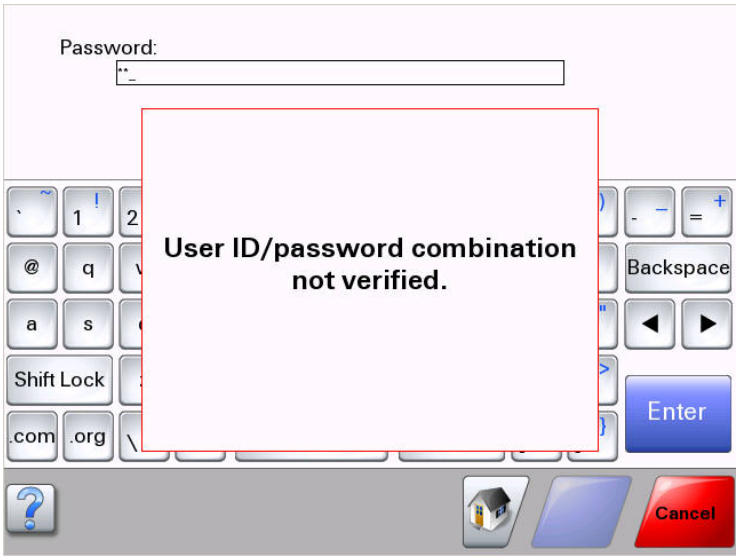
2.4.2 User Authentication

The TOE's display interface allows access to the following types of scan-based operations to touch screen users: scan-to-fax, scan-to-copy, scan-to-USB, and scan-to-email. The TOE's display interface also allows access to the print-from-USB operation to touch screen users. Each of these operations is restricted with the User Authentication function, which requires the touch screen user's credentials to be submitted and validated before the TOE gives the touch screen user access to the operation. The authentication is performed against a set of touch screen user accounts that are maintained by the TOE. The TOE touch screen user account passwords are configurable and are a minimum of six characters in length.

If for any reason the User ID and Password provided by the touch screen user do not match a set of credentials in the list of touch screen user accounts, access is denied and the touch screen user is prompted again.

After three successive failed attempts at authentication, the touch screen user is notified with the GUI represented in the following figure. The system does not lock out the touch screen user account.

Figure 2. Three Failed Attempts Notification.



Note that no identification or authentication is performed for network print users or inbound fax users. These roles may transmit (via the local area network or fax line respectively) data to be printed on the embedded printer, and have no access to any other security-relevant functions.

2.4.3 Device Configuration Protection

The TOE's System Administrator password is configurable and is a minimum of eight characters in length. The administrative account cannot be deleted, or disabled. There are no means to add any system administrator authority to touch screen user accounts.

When a remote session is established to the MFP via HTTPS, the user has access to a device status page. If access is attempted to any of the configuration menus, the user is prompted to provide the System Administrator password. If an invalid Password is specified, access is denied and the user is prompted again.

System Administrators can perform such tasks as creating user accounts and updating user passwords. The MFP device includes parameters that can be configured by an administrator. The Device Configuration Protection function restricts the ability to configure those parameters by requiring authentication against the TOE's administrative account.

The configurable settings that control the behaviour of the MFP related to scanning, email, authentication, and all other major functions can only be modified after authentication with the TOE's administrative credentials.

To invoke the Hard Disk Sanitization function, the System Administrator uses the Touch Panel with a special key sequence on startup of the MFP. The user is prompted to provide the System Administrator password. If an invalid password is specified, access is denied and the user is prompted again.

Management of the MFP occurs primarily via remote access utilizing HTTPS. These sessions provide protection against disclosure and modification via SSL v2 and v3 and TLS v1.

2.4.4 Hard Disk Encryption

All user data files stored on the hard disk are encrypted using the AES algorithm and a 128-bit key. This operation is transparent to the users, as the files are automatically encrypted when saved and automatically decrypted when retrieved. The encryption key is specific to the MFP and hard disk. All user data files on the hard disk will be lost as a result of the following actions:

A) Disabling the hard disk encryption feature - the encryption key is destroyed

B) Enabling the hard disk encryption feature when it is already enabled - a new encryption key is generated; the previous key is destroyed

C) Removing the hard disk from the MFP and inserting it into a different MFP - the encryption key is stored in the MFP, not on the hard disk

2.4.5 Hard Disk Sanitization

When directed by the System Administrator, the TOE will sanitize the hard disk. This operation is meant to be used when the system is taken out of service or removed from a secure location. The operator has the option of performing a single overwrite pass with all zeros or seven overwrite passes with different bit patterns followed by a verify pass. This functionality ensures that any data present on the hard disk could not be recovered even if the encryption key was compromised.

2.4.6 TSF Self Protection

The MFP protects itself by ensuring that security functions may not be bypassed by activities within the TSC and by implementing security domains that protect it from interference and tampering by untrusted subjects within the TSC.

The MFP maintains separate memory spaces for its various processes, and uses well-defined interfaces for interprocess communication to control interactions between the processes. Remote login to a command prompt and the remote execution of MFP services is not allowed.

The TSF Self Protection function is inherent in the architecture of the system, and does not rely on external interfaces or explicit activation.

2.5 TSF Data

The following table defines the TSF data.

Table 2 - TSF Data

Category	Item	Description
Authentication Data	Administrator Password	Used by the administrator to authenticate in order to gain access to system management web pages.

Category	Item	Description
	User ID	Identifies a specific user authorized to perform operations via the Touch Screen.
	User Password	Used to authenticate a specific user attempting to perform operations via the Touch Screen.
Subject Security Attributes	Touch Screen Permissions	Permissions to access the various Touch Screen functions are defined on a per-function basis.
TSF Data	Hard Disk Encryption Key	The key used to encrypt and decrypt all data on the hard disk.

2.6 User Data

The User Data operated on by the TOE is any data that is stored on the hard disk.

2.7 Rationale for Non-Bypassability and Separation for the TOE

The TOE is a device that includes firmware that executes on top of an underlying hardware system. Together, the firmware application and underlying hardware make up the TOE.

The TOE is protected from interference. The firmware is not a general purpose operating system and does not allow generic users to introduce new processes or executable code to the system. Arbitrary entry into the TOE is not possible and therefore the TSF is protected against external interference by untrusted objects.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through role based access control, the TSF is protected from corruption or compromise.

2.8 Lexmark X646dte, X646e, X646ef, X772e, X850e, X852e, X854e, X940e and X945e MFPs Evaluated Configuration

2.8.1 Operational Environment

The evaluated configuration will be as detailed below:

A) Internal User Authentication is selected for the authentication mode.

B) All scan and print operations accessible via the touch screen operator panel require users to successfully identify and authenticate before proceeding.

C) HTTPS is enabled; HTTP is disabled.

D) All security-relevant system administrator functions other than Hard Disk Sanitization occur through a browser using HTTPS. Access to the device configuration menus other than Hard Disk Sanitization through the Touch Screen is disabled.

E) The Advanced Password is configured for all system administration functions. Access to specific configuration pages available through HTTPS requires knowledge of the Advanced Password to gain access. Configuration of the specific pages is detailed in the following table.

Table 3 - System Administration Web Page Access

Web Page	Description	Controlled Access?
Device Status	Displays device information including Tray size and capacity, toner status, and output bin status. Nothing on the TOE can be configured from this page.	No
Scan Profile	Allows the administrator to create a scan profile on the TOE that enables a user to scan a document back to their local computer.	Yes
Reports	Contains device reports.	Yes
Links & Index	Contains links to public Lexmark.com websites that allow operators to get technical support, order supplies, and get other general interest information. This page also contains an index of links to all the configuration pages contained under the configuration menu. All of the index links use the same security settings as the configuration menu	Yes
Applications	Displays any extra Lexmark applications installed on the TOE. In the evaluated configuration, there are no applications installed and this page is basically empty.	Yes
Order Supplies	Direct link to the Lexmark.com homepage.	No
Configuration	Provides links to all the configuration submenus.	No, but access to all of the configuration submenus is restricted

F) FTP server functionality is disabled.

G) The NetWare protocol is disabled.

H) The AppleTalk protocol is disabled.

I) The DLC protocol is disabled.

J) The MVP management protocol is disabled.

K) SNMP is disabled.

2.8.2 Functionality Not Included in the Evaluation

The following functionality is present in the MFPs but was not included in the evaluation:

A) Integration with external authentication servers

B) Restricted server list

C) Embedded solutions

D) 802.1x authentication

E) Confidential print

F) IPSec support

G) Integration with external time servers

H) Ability to update the firmware

I) Importing configuration files

J) Sending email alerts

K) Touch Screen Lock

CHAPTER 3

3. TOE Security Environment

This chapter identifies Threats (T), Assumptions (A), and Organisational Security Policies (P) related to the TOE. Threats are those that are addressed by the TOE and/or operating environment. Assumptions detail the expected environment and operating conditions of the system. Organisational Security Policies are specific rules, procedures, or practices that are part of the TOE.

3.1 Threats

The threats identified in the following table sections are addressed by the TOE and/or Operating Environment.

Table 4 - Threats

Name	Description
T.ACCESS	An unauthorized individual may attempt to gain access to the TOE functions and to TOE resources through either malicious or accidental means.
T.FAXLINE	A hostile entity may attempt to gain unauthorized access through a phone connection to TOE resources, or TOE connected networks to retrieve data of value.
T.NOAUTH	An authorized user may attempt to gain unauthorized access to TOE security functions.

3.2 Assumptions

The assumptions fall into three groups. They are personnel assumptions, physical environment assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.

B) Physical environment assumptions describe characteristics of the non-IT environment within which the system is deployed.

C) IT environment assumptions describe the technology environment within which the TOE is operating.

Table 5 - Assumptions

Name	Description
A.NOEVIL	System Administrators are not evil, follow the Lexmark MFP Administrative Guidance before exercising security management functions related to the system, and do not attempt to attack or subvert the TOE and its policy. System Administrators are responsible for managing the TOE and the security of the information it contains.
A.LOCATE	The processing resources of the TOE will be located within non-hostile facilities that will prevent unauthorized physical access by hostile individuals who could compromise the TSF.

3.3 Organisational Security Policies

There are no Organisational Security Policies identified for this TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

Table 6 - Objectives for the TOE

Name	Description
O.ACCESS	The TOE identifies and authenticates users prior to allowing access to TOE functions and resources with the exception of access to the MFP status page via HTTPS, network print, and fax print operations.
O.DATAPROTECT	The TOE will protect data on the hard disk from unauthorized access by malicious agents who gain access physical access to the disk.
O.FAX_DESIGN	The design of the TOE shall prohibit a user from hijacking the TOE and using it to attack the network connected to the TOE via the fax modem.
O.MANAGE	The TOE provides access by authenticated administrators to TOE resources and management functions.
O.NOTAMPER	The TOE must protect against interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions.
O.PWDPROTECT	The TOE protects the user and system administrator passwords by providing only obscured feedback when entering.
O.RESTRICT	The design of the TOE shall prohibit a user from modifying TOE data or configuration internal to the TOE via the fax modem.

4.2 Security Objectives for the Operating Environment

Table 7 - Objectives for the Environment

Name	Description
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

CHAPTER 5

5. IT Security Requirements

This section contains the IT security requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 TOE Security Functional Requirements

The security functional requirements are described in detail in the following subsections. These requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of the security functional requirements identified as explicitly stated and the items within the security functional requirements identified as operations that are TOE specific. The following table identifies the security functional requirements of the TOE (both derived verbatim from Part 2 of the CC and explicitly stated).

The CC defines four operations on security functional requirements. The font conventions listed below identify the conventions for the operations defined by the CC.

A) Assignment: indicated in italics

B) Selection: indicated in underlined text

C) Assignments within selections: indicated in italics and underlined text

D) Refinement: indicated with **bold** text

The following table summarizes the security functional requirements claimed.

Table 8 - Security Functional Requirements (SFRs)

Security Functional Requirements	
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FIA_UAU.1	Timing of Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of Identification
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation

The following table summarizes the explicitly stated security functional requirements claimed.

Table 9 - Explicitly Stated Security Functional Requirements

Explicitly Stated Security Functional Requirements	
FDP_DRM_EXP.1	Data Remanence
FPT_FAX_EXP.1	Fax Communications Control

5.1.1 Cryptographic Support (FCS)

5.1.1.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm used by the *dev/urandom* system call and specified cryptographic key size of *128 bits* that meet the following: *N/A*.

5.1.1.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2*.

5.1.1.3 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform *the operations described below* in accordance with a specified cryptographic algorithm *multiple algorithms in the modes of operation described below* and cryptographic key sizes *multiple key sizes described below* that meet the following *multiple standards described below*:

Table 10 - Cryptographic Operations

Operation	Algorithm (mode)	Certificate	Key Size in Bits	Standards
Encryption and decryption	AES (CBC)	algorithm certificate 565	128, 256	FIPS 197
	DES (CBC)	tested by CCTL	56	FIPS 46-3
	RC2 (CBC)	tested by CCTL	40 to 128	RFC 2268
	RC4 (CBC)	tested by CCTL	40 to 128	
	TDES (CBC)	tested by CCTL	168	FIPS 46-3
Hash	MD5	tested by CCTL	n/a	RFC 1321
	SHS (SHA-1)	tested by CCTL	n/a	FIPS 180-2
Key agreement	Diffie-Hellman (ephemeral-static)	tested by CCTL	2048	RFC 2631
Key wrapping	RSA	tested by CCTL	128	ANSI X9.31

5.1.2 Class FIA: Identification and Authentication

5.1.2.1 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *network print and fax print operations, access to the MFP status page via HTTPS* on behalf of the user to be performed before the user is authenticated.

Application Note: *Fax print operations refer to the ability of inbound fax users to send fax files to be printed on the printer associated with the scanner unit. Network print operations refer to print jobs sent by network attached users to be printed.*

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.

Application Note: *Users other than System Administrators may access the TOE via HTTPS to view status information for the MFP, so they are using the same security functionality that protects the administrator communication.*

5.1.2.2 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the user while the authentication is in progress.

5.1.2.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *network print and fax print operations, access to the MFP status page via HTTPS* 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.

Application Note: *Users other than System Administrators may access the TOE via HTTPS to view status information for the MFP, so they are using the same security functionality that protects the administrator communication.*

5.1.3 Class FMT: Security Management

5.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to disable, enable, modify the behaviour of the functions**:** *Touch Screen User Authentication, Device Configuration Protection function, Hard Disk Encryption, and Hard Disk Sanitization* to *the System Administrator.*

5.1.3.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *create*, query, modify, delete, and clear the *touch screen user password and system administrator password* to *the System Administrator.*

5.1.3.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *creating touch screen user accounts; modifying touch screen user password and system administrator password; and invoking Hard Disk Sanitization.*

5.1.3.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *System Administrator, Touch Screen Users, Inbound Fax Users, and Network Print.*

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

5.1.4 Protection of the TSF (FPT)

5.1.4.1 FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.4.2 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5 Explicitly Stated Security Functional Requirements

The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements that are not currently defined in Part 2 of the *Common Criteria for Information Technology Security Evaluation*.

5.1.5.1 FDP_DRM_EXP.1 Data Remanence

FDP_DRM_EXP.1.1 The TSF shall overwrite the entire MFP hard disk to ensure that data remanence is destroyed.

FDP_DRM_EXP.1.2 The TSF shall perform the overwrite operation on demand by an Administrator.

5.1.5.2 FPT_FAX_EXP.1 Fax Communications Control

FPT_FAX_EXP.1.1 The TSF shall ensure that all data transmitted or received via fax is associated only with the transmission or reception of facsimile jobs.

FPT_FAX_EXP.1.2 The TSF shall ensure that user data stored in the TOE is inaccessible to exploitations via the fax port.

FPT_FAX_EXP.1.3 The TSF shall ensure that the TOE cannot be configured or managed via the fax port.

5.2 Security Functional Requirements for the IT Environment

No SFRs are levied on the IT Environment.

5.3 Rationale for Explicitly Stated Security Functional Requirements

This section provides the rationale for the explicitly stated security functional requirements and demonstrates how each security objective is enforced by the security functional requirements. The explicitly stated security functional requirements identify security functional requirements that are not currently defined in Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

The following table provides the rationale for choosing explicitly stated Security Functional Requirements.

Table 11 - Explicitly Stated Security Functional Requirements

Explicitly Stated SFR	Rationale
FDP_DRM_EXP.1	The CC does not have any function for dealing with data remanence. FDP was chosen as the class because the function involves protection of user data.
FPT_FAX_EXP.1	FPT was chosen as the class because the security function involves protection of the TSF. The security function is designed in the TOE and provides separation between fax operations and other TSF but does not fully implement domain separation or reference mediation.

5.4 Rationale for Security Functional Requirements and Dependencies

The following table lists the claimed TOE security functional requirements and their dependencies.

Table 12 - Rationale for Security Functional Requirements and Dependencies

Claim	Hierarchical to	Dependencies	Rationale
FCS_CKM.1	None	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	 Satisfied Satisfied Not required since the keys are automatically generated by the TOE.
FCS_CKM.4	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	 The key is generated from a random number, addressed by FCS_COP.1 Not required since the keys are automatically generated by the TOE.
FCS_COP.1	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	 The key is generated from a random number, addressed by FCS_COP.1 Satisfied Not required since the keys are automatically generated by the TOE.
FDP_DRM_EXP.1	None	None	n/a
FIA_UAU.1	None	FIA_UID.1	Satisfied
FIA_UAU.7	None	FIA_UAU.1	Satisfied
FIA_UID.1	None	None	n/a
FMT_MOF.1	None	FMT_SMR.1	Satisfied
FMT_MTD.1	None	FMT_SMR.1	Satisfied
FMT_SMF.1	None	None	n/a
FMT_SMR.1	None	FIA_UID.1	Satisfied
FPT_FAX_EXP.1	None	None	n/a
FPT_RVM.1	None	None	n/a
FPT_SEP.1	None	None	n/a

5.5 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 as defined by Part 3 of the CC. These assurance requirements are summarized in the following table.

Table 13 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.6 Rationale for TOE Security Assurance Requirements

EAL2 was chosen to provide a basic level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low and the product will have undergone a search for obvious flaws.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

The TOE meets the assurance requirements for EAL2. The CC states that EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 was chosen to provide a basic level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low and the product will have undergone a search for obvious flaws. EAL2 was also chosen based on the statement of the security environment (assumptions, threats and organisational policy) and the security objectives

defined in this ST. EAL2 is, therefore, applicable in those circumstances where developers or users require a basic level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

5.7 TOE Strength of Function Claim

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, August 1999, defines “Strength of Function (SOF)” in terms of the minimum efforts assumed necessary to defeat the expected security behaviour of a TOE security function.

The only probabilistic or permutational mechanism in the TOE is the authentication mechanisms used for the Administrative Password and Touch Screen User Authentication Password.

The claimed minimum strength of function is SOF-basic. FIA_UAU.1 and FIA_UID.1 are the only TOE security functional requirements that depend on this permutational function.

5.8 Rationale for Strength of Function Claim

5.8.1 System Administrator Password via Touch Panel

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_UAU.1 and FIA_UID.1 contain a permutational function requiring a SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST and the strength of the minimum password length. Based on the SOF Analysis below, the SOF-basic strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

The MFP Administrative password is a minimum of eight characters in length, and includes both alphabetic characters and non-alphabetic characters. Passwords must not be dictionary words.

A password length of eight was analyzed since it is the minimum value. One second was used as a conservative length of time required to enter an ID and Password into the Lexmark MFP. This analysis assumes passwords will not be easy to guess since they are specified by a qualified administrator. Based on these assumptions, the password space is calculated as follows:

Password length: p = 8

Unique characters: c = 67

Seconds per attempt: s = 1

Average length of successful attack in years =

= (s * c^p seconds) / (2 * (60 * 60 * 24 seconds per day))

= (1 * 67^8) / (2 * 60 * 60 * 24)

= 406067677556641 / 172800 days

= 2349928689 days / 365 days per year

= 6438160 years

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘Low’.

5.8.2 System Administrator Password via External Webpage

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_UAU.1 and FIA_UID.1 contain a permutational function requiring a SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST and the strength of the minimum password length. Based on the SOF Analysis below, the SOF-basic strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

The MFP Administrative password is a minimum of eight characters in length, and includes both alphabetic characters and non-alphabetic characters. Passwords must not be dictionary words.

A password length of eight was analyzed since it is the minimum value. 5000 attempts per second were assumed via the network interface. This analysis assumes passwords will not be easy to guess since they are specified by a qualified administrator. Based on these assumptions, the password space is calculated as follows:

Password length: p = 8

Unique characters: c = 67

Seconds per attempt: s = .0002

Average length of successful attack in years =

= (s * c^p seconds) / (2 * (60 * 60 * 24 seconds per day))

= (.0002 * 67^8) / (2 * 60 * 60 * 24)

= 81213535511 / 172800 days

= 469986 days / 365 days per year

= 1287 years

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘Low’.

5.8.3 User Authentication Password

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_UAU.1 and FIA_UID.1 contain a permutational function requiring a SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST and the strength of the minimum password length. Based on the SOF Analysis below, the SOF-basic strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

A password length of six was analyzed since it is the minimum value. One second was used as a conservative length of time required to enter an ID and Password into the Lexmark MFP. This analysis assumes passwords will not be easy to guess since they are specified by a qualified administrator. Based on these assumptions, the password space is calculated as follows:

Password length: p = 6

Unique characters: c = 67

Seconds per attempt: s = 1

Average length of successful attack in years =

= (s * c^p seconds) / (2 * (60 * 60 * 24 seconds per day))

= (1 * 67^6) / (2 * 60 * 60 * 24)

= 90458382169 / 172800 days

= 523486 days / 365 days per year

= 1434 years

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘Low’.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the TOE Security Functional Requirements (SFRs). Additional detail related to the Security Function-to-SFR correlation is found in later sections.

6.1.1 Fax Communications Control

The Fax Communications Control security function assures that the information on the TOE, and the information on the network to which the TOE is attached, is not exposed through the phone line that provides connectivity for the analog fax function. This function assures that only printable documents are accepted via incoming fax connections, and that the only thing transmitted over an outgoing fax connection is the document that was submitted for faxing.

The Fax Communications Control security function is inherent in the design of the system, and is not explicitly activated. Control of the fax functionality is incorporated directly into the TOE's firmware. The fax chip that sends and receives data over the phone line is directly controlled by the TOE firmware. The modem chip is in a mode that's more restrictive than Class 1 mode, and relies on the TOE firmware for composition and transmission of fax data. The TOE firmware explicitly disallows the transmission of frames in data mode and allows for the sending and receiving of facsimile jobs, only. There is no mechanism by which telnet, FTP, or other network protocols can be sent or received over the analog fax line.

The MFP uses a Conexant SFX336 Fax Modem which has no capability of establishing a data connection. This modem is on a separate card from the network adapter to provide separation between the interfaces and is only capable of sending and receiving fax data. There is no way for the modem and the network adapter to communicate directly with one another. The modem is designed only for fax communications, thus preventing any type of remote configuration or management of the TOE over the fax line.

In addition, the firmware which controls the communication between the SFX336 and the rest of the TOE is also designed only for fax communications. Aside from passing facsimile data representing page images to be faxed to the modem or passing incoming pages to the TOE to be printed, there is no method of data transfer between the fax modem and the TOE. This insures that the fax function and the administrative functions remain separate from one another.

6.1.2 User Authentication

The TOE's display interface allows access to the following types of scan-based operations to touch screen users: scan-to-fax, scan-to-copy, scan-to-USB, and scan-to-email. The TOE's display interface also allows access to the print-from-USB operation to touch screen users. Each of these operations is restricted with the User Authentication function. The User Authentication function requires the touch screen user's credentials (identity and password) to be submitted and validated before the MFP gives the touch screen user access to the operation. The authentication is performed

against a set of touch screen user accounts that are stored on the MFP device. Note that the authentication requirement is applied to all of the MFP's scan-based and USB operations in the evaluated configuration. All passwords are obscured when being entered. This security function contains a permutational mechanism, the user password.

6.1.3 Device Configuration Protection

The TOE supports a system administrator account. The administrative account cannot be deleted or disabled. There are no means by which to add any administrative authority to user accounts. System administrators can perform such tasks as creating user accounts and updating user passwords.

The MFP device includes parameters that can be configured by an administrator. The Device Configuration Protection function restricts the ability to configure those parameters by requiring authentication against the MFP's administrative account.

The configurable settings that control the behavior of the MFP related to scanning, email, authentication, and all other major functions can only be modified after authenticating with the MFP's administrative credentials. This security function contains a permutational mechanism, the device administrator password.

Device configuration is performed via a web browser. The web browser interface requires HTTPS to protect against disclosure and modification of data. TLSv1, SSLv2, and SSLv3 are accepted from connecting clients. TLSv1 is the preferred method, stepping down to SSLv3 and finally SSLv2 as required. For these protocols, the random number generator in the TOE is used in conjunction with the cipher suites listed in the following table. HTTPS is a server certificate only security path. The server (the TOE) will present its device certificate for the client (the remote web client) to authenticate. No client certificate is involved. Once the session ends, the key used for that session is zeroized.

Table 14 - TLS/SSL Cipher Suites Supported

Protocol	Supported Cipher Suites
TLSv1	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_DES_CBC_SHA
	TLS_RSA_WITH_RC4_128_MD5
	TLS_RSA_WITH_RC4_128_SHA
SSLv3	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_DES_CBC_SHA
	TLS_RSA_WITH_RC4_128_MD5
	TLS_RSA_WITH_RC4_128_SHA

SSLv2	SSL_CK_RC4_128_EXPORT40_WITH_MD5
	SSL_CK_RC4_128_WITH_MD5

6.1.4 Hard Disk Encryption

All user data saved on the Hard Disk is encrypted using 128-bit AES. The types of data saved on the Hard Disk (and therefore encrypted) include buffered job data, held jobs, images referenced by other jobs, and macros. The contents of each file are automatically encrypted 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. This security function operates transparently to users and is always enabled in the evaluated configuration.

A common key is used to encrypt all files. A random number is used as the key; the key is determined when this function is enabled during installation. The key is saved in internal non-volatile random access memory (NVRAM), enabling information on the hard disk to be decrypted across reboots. The key is zeroized if this function is disabled.

The encryption key is specific to the MFP and hard disk. All user data files on the hard disk will be lost as a result of the following actions:

A) Disabling the hard disk encryption feature - the encryption key is zeroized

B) Enabling the hard disk encryption feature when it is already enabled - a new encryption key is generated; the previous key is zeroized

6.1.5 Hard Disk Sanitization

The system administrator may initiate Hard Disk Sanitization to ensure that all data has been permanently eliminated from the Hard Disk. This process provides additional protection beyond Hard Disk Encryption against data disclosure if the Hard Disk should be acquired by unauthorized agents, since no residual data remains on the Hard Disk to be recovered.

Hard Disk Sanitization sanitizes all user data from the Hard Disk. The process is initiated via the Touch Panel by the system administrator. The system administrator has the option of performing a single overwrite pass with all zeros or seven overwrite passes with different bit patterns followed by a verify pass. While Hard Disk Sanitization is in process, the MFP should be disconnected from the network and fax line. Upon successful completion, the system administrator is notified on the Touch Panel.

Hard Disk Sanitization never occurs automatically; it must be manually initiated by the system administrator.

6.1.6 TSF Self Protection

The system protects itself by ensuring that security functions may not be bypassed by activities within the TSC and by implementing security domains that protect it from interference and tampering by untrusted subjects within the TSC.

6.2 Security Assurance Measures and Rationale

The assurance measures provided by the TOE satisfy all of the assurance requirements, as listed in the following table. A reference is provided between each TOE assurance requirement and the related vendor documentation that satisfies that requirement.

Table 15 - Assurance Measures and Rationale

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Configuration Management Plan	Lexmark Configuration Management Practices This requirement is met by documentation describing the Configuration Management system used during the development of the TOE. The Configuration Management Plan describes the CM measures to ensure that the configuration items are uniquely identified and changes are accurately tracked. The documentation describes the processes and procedure followed and automated tools that are utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE.
ADO_DEL.1	Delivery Procedures	Delivery and Installation Documentation for Lexmark Multifunction Printers This requirement is met by documentation describing the delivery of the TOE. The delivery and operations documentation describes the methods and procedures used to distribute the TOE securely and verify its integrity.
ADO_IGS.1	Installation, Generation and Start-up Documentation	Delivery and Installation Documentation for Lexmark Multifunction Printers This requirement is met by documentation describing the Installation, Generation and Start-up of the TOE. This documentation describes procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. It provides authorized administrator and user guidance on how to perform the TOE security functions. It also provides warnings to authorized administrators and users about actions that can compromise the security of the TOE.

Assurance Component	Documentation Satisfying Component	Rationale
ADV_FSP.1	Functional Specification	Security Functional Specification for Lexmark Multifunction Printers This requirement is met by the Functional Specification for the TOE. The Functional Specification provides all interface specifications fully describing all interfaces to the TSF.
ADV_HLD.1	High Level Design Document	High Level Design Specification for Lexmark Multifunction Printers These documents contain a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	Security Target, Functional Specification, and related Design Documentation	Development Representation Correspondence Document The correspondence between the TOE security functions and the high-level design subsystems is described in this document.
AGD_ADM.1	Administrator Guidance Documentation	Important Information For Common Criteria EAL2 Compliant Operation This requirement is met by the Administration Guidance documentation. The Administrative Guidance documentation describes the interfaces and procedures that are used by the administrator to operate and administer the TOE in a secure manner. It also describes the security functions and interfaces that are used to configure the functions.
AGD_USR.1	User Guidance documentation	Important Information For Common Criteria EAL2 Compliant Operation The User Guidance describes the interfaces and procedures that are used to operate the TOE. This guidance documents the security functions, warnings and the interfaces that are utilized to configure the security functions. It also describes actions that can compromise the security of the TOE.

Assurance Component	Documentation Satisfying Component	Rationale
ATE_COV.1	Functional Specification, Test documentation and Test Coverage Analysis.	Functional Testing of Lexmark Multifunction Printers The TOE test documentation describes how all security relevant APIs are tested, and specifically describes all test cases and variations necessary to demonstrate that all security checks and effects related to the API are correctly implemented. The test documentation provides correspondence between the security-relevant APIs and applicable tests and test variations that are described in the Functional Specification The test documentation describes the actual tests, procedures to successfully execute the tests, and expected results of the tests. The test documentation analysis includes results in the form of logs resulting from completely exercising all of the security test procedures.
ATE_FUN.1	Functional Specification, Test documentation and procedures.	Functional Testing of Lexmark Multifunction Printers The TOE test documentation describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
ATE_IND.2	Developer Test Documentation, Evaluation Lab Independent Testing and Evaluation Deliverables.	Functional Testing of Lexmark Multifunction Printers This assurance requirement is met by the functional and penetration tests performed and includes test results which serve as Evaluation Deliverables. A TOE suitable for testing has also been provided.
AVA_SOF.1	Strength of Function Analysis	Strength of Function Analysis This assurance requirement is met by the documented Strength of Function Analysis. The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct.
AVA_VLA.1	Vulnerability Analysis, and Evaluation Deliverables	Developer Vulnerability Analysis Document This assurance requirement is met by the Vulnerability Analysis, evaluation deliverables and a copy of the TOE suitable for testing. The Vulnerability Analysis identifies the vulnerabilities in the TOE. The analysis provides the status of each identified vulnerability and demonstrates that a given vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks. Misuse Analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional requirements.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 16 - Threats and Assumptions to Security Objectives Mapping

	O.ACCESS	O.DATAPROTECT	O.FAX_DESIGN	O.MANAGE	O.NOTAMPER	O.PWDPROTECT	O.RESTRICT	OE.ENVIRON	OE.INSTALL	OE.NOEVILADMIN
T.ACCESS	X	X			X	X				
T.FAXLINE			X				X			
T.NOAUTH	X									
A.NOEVIL										X
A.LOCATE								X	X	

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 17 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ACCESS	O.ACCESS addresses T.ACCESS because the TOE identifies and authenticates users prior to allowing access to TOE functions and resources and protects unauthorized access to information by unauthorized individuals through either malicious or accidental means. O.DATAPROTECT addresses T.ACCESS because it provides protection against disclosure for user data stored within the TOE. O.NOTAMPER addresses T.ACCESS by ensuring the TOE functions can not be tampered with or bypassed. O.PWDPROTECT addresses T.ACCESS by ensuring that user and system administrator passwords are never viewable in clear text.

T.TYPE	Security Objectives Rationale
T.FAXLINE	O.FAX_DESIGN addresses T.FAXLINE by incorporating sound security design principles in the construction of the TOE thereby ensuring that user data stored in the TOE and outside the TOE is inaccessible to exploitations via the fax port and that the TOE is impervious to hijacking via the fax port. O.RESTRICT addresses T.FAXLINE by ensuring that fax operations are separate and distinct from other TOE operations and TOE data.
T.NOAUTH	O.ACCESS addresses T.NOAUTH and T.ACCESS as it ensures that people attempting to access TOE security management functions are first identified and authenticated.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 18 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.NOEVIL	OE.NOEVILADMIN addresses the assumption by ensuring administrators are not evil and adhere to the guidance provided for the TOE.
A.LOCATE	OE.ENVIRON and OE.INSTALL address the assumption by ensuring the TOE is properly installed in an appropriate location with restricted physical access.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 19 - SFRs to Security Objectives Mapping

	O.ACCESS	O.DATAPROTECT	O.FAX_DESIGN	O.MANAGE	O.NOTAMPER	O.PWDPROTECT	O.RESTRICT
FCS_CKM.1		X					
FCS_CKM.4		X		X			
FCS_COP.1		X		X			
FDP_DRM_EXP.1		X					
FIA_UAU.1	X						
FIA_UAU.7						X	
FIA_UID.1	X						
FMT_MOF.1				X			
FMT_MTD.1				X			

	O.ACCESS	O.DATAPROTECT	O.FAX_DESIGN	O.MANAGE	O.NOTAMPER	O.PWDPROTECT	O.RESTRICT
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_FAX_EXP.1			X				X
FPT_RVM.1					X		
FPT_SEP.1					X		

The following table provides the detail of TOE security objective(s).

Table 20 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	FIA_UAU.1 and FIA_UID.1 support O.ACCESS by ensuring that only access to the MFP status page via HTTPS, network print and fax print can be performed before user authentication.
O.DATAPROTECT	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 support this objective by providing the ability to generate and destroy keys which are used with the AES algorithm to encrypt all user data stored on the hard disk. FDP_DRM_EXP.1 supports this objective by providing the ability to sanitize all user data that had been stored on the hard disk.
O.FAX_DESIGN	FPT_FAX_EXP.1 supports this objective by imposing strict limitations on the functionality provided via the Fax interface.
O.MANAGE	FCS_CKM.4 supports this objective by zeroizing the key used to protect the HTTPS session after the session terminates. FCS_COP.1 supports this objective by providing key agreement and encryption for secure interactions with the System Administrator via HTTPS. FMT_MOF.1 supports O.MANAGE by ensuring that only system administrators have the capability to disable, enable, or modify the behaviour of the security functions. FMT_MTD.1 supports O.MANAGE by associating operations such as the ability to create, query, modify, delete, and clear security-relevant TSF data with the authorized roles. FMT_SMF.1 supports O.MANAGE by defining the set of security functions available on the TOE. FMT_SMR.1 supports O.MANAGE by ensuring that the security management functions are authorized to the proper roles.
O.NOTAMPER	FPT_RVM.1 supports O.NOTAMPER by ensuring the TSF cannot be bypassed by actions within the TSC. FPT_SEP.1 supports O.NOTAMPER by ensuring the TSF cannot be interfered with by subjects within the TSC.
O.PWDPROTECT	FIA_UAU.7 supports O.PWDPROTECT by ensuring that only obscured feedback is provided to the user when entering passwords.
O.RESTRICT	FPT_FAX_EXP.1 supports this objective by imposing strict limitations on the functionality provided via the Fax interface.

8.2.2 Security Assurance Requirements Rationale

8.2.2.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL2. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 21 - Assurance Measures

Component ID	Rationale
ACM_CAP.2	The following CM procedures are described in this documentation: Use of the automated tool for revision control Use of documented procedures for product builds Use of documented procedures for product test Use of documented procedures for release to manufacturing Use of documented procedures for distribution to customers List of configuration items and evidence that the automated tool maintains them. .
ADO_DEL.1	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	This document describes the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	This document describes the purpose and method of use of all external TSF interfaces and completely represents the TSF.
ADV_HLD.1	These documents contain a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in this document.
AGD_ADM.1	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	Guidance to non- administrative users is effectively supported by the listed documentation for this requirement
ATE_COV.1	These documents describe the functional and penetration test performed and their results.
ATE_FUN.1	These documents describe the functional and penetration test performed and their results.
ATE_IND.2	These documents describe the functional and penetration test performed and their results.
AVA_SOF.1	These documents include a strength of function analysis to support the SOF-basic claim.
AVA_VLA.1	These documents describe the vulnerability analysis performed and the results of the analysis.

8.2.2.2 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 22 - SFRs to TOE Security Functions Mapping

	Fax Communication Control	User Authentication	Device Configuration Protection	Hard Disk Encryption	Hard Disk Sanitization	TSF Self Protection
FCS_CKM.1				X		
FCS_CKM.4			X	X		
FCS_COP.1			X	X		
FDP_DRM_EXP.1					X	
FIA_UAU.1		X	X			
FIA_UAU.7		X	X			
FIA_UID.1		X	X			
FMT_MOF.1			X			
FMT_MTD.1			X			
FMT_SMF.1			X			
FMT_SMR.1			X			
FPT_FAX_EXP.1	X					
FPT_RVM.1						X
FPT_SEP.1						X

Table 23 - SFR to SF Rationale

SFR	SF and Rationale
FCS_CKM.1	The Hard Disk Encryption security function addresses this SFR by using the random number generator to create an AES key.

SFR	SF and Rationale
FCS_CKM.4	The Hard Disk Encryption security function addresses this SFR by zeroizing the key if encryption is disabled. The Device Configuration Protection security function addresses this SFR by zeroizing the key when an HTTPS session terminates.
FCS_COP.1	The Hard Disk Encryption security function addresses this SFR by using the random number generator and AES for encryption of data on the hard disk. The Device Configuration Protection addresses this SFR by using key agreement and encryption for TLS/SSL.
FDP_DRM_EXP.1	The Hard Disk Sanitization security function addresses this SFR by performing disk wiping when directed by the System Administrator.
FIA_UAU.1	The User Authentication security function supports FIA_UAU.1 by performing the I&A function for Touch Screen operations. The Device Configuration Protection security function supports FIA_UAU.1 by performing the I&A function for administrative access and allowing access to the status page prior to I&A.
FIA_UAU.7	The User Authentication and Device Configuration Protection security functions support FIA_UAU.7 by providing obscured feedback to the user while the authentication is in progress.
FIA_UID.1	The User Authentication security function supports FIA_UID.1 by performing the I&A function for Touch Screen operations. The Device Configuration Protection security function supports FIA_UID.1 by performing the I&A function for administrative access and allowing access to the status page prior to I&A.
FMT_MOF.1	The Device Configuration Protection security function supports FMT_MOF.1 by ensuring that only system administrators can access Security Management Functions.
FMT_MTD.1	The Device Configuration Protection security function supports FMT_MTD.1 by restricting operations that can be performed on TSF data to the system administrator.
FMT_SMF.1	The Device Configuration Protection supports FMT_SMF.1 by ensuring that the following security management functions can be performed and maintained: creating touch screen user accounts; modifying user and system administrator passwords; and invoking Hard Disk Sanitization.
FMT_SMR.1	The Device Configuration Protection function support FMT_SMR.1 by ensuring that TSF management operations are limited to the administrator role
FPT_FAX_EXP.1	The Fax Communication Control security function supports FPT_FAX_EXP.1 by ensuring that all of the data sent or received from the MFP via the fax interface is associated only with the transmission (inbound or outbound) of facsimile jobs. The TOE ensures that no other sort of data is transmitted or received through the fax connection.
FPT_RVM.1	The TSF Self Protection security function supports FPT_RVM.1 by ensuring that TSP enforcement is always invoked before security functions within the TSC are allowed to proceed.
FPT_SEP.1	The TSF Self Protection security function supports FPT_SEP.1 by ensuring that the TSF is protected against interference and tampering by untrusted subjects.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

8.5 Strength of Function Rationale

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, SOF-basic was chosen.