Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b Security Target
March 28, 2006
Document No. F2-0206-008(1)

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, MD 21046-2587

Phone: 301-498-0150

Fax: 301-498-0855

Document Introduction

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite N
Columbia, Maryland 21046-2587

Prepared For:

Lexmark, Inc.
740 New Circle Road NW
Lexington, KY 40511

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b. 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.

Revision History

Rev	Date	Description
	February 23, 2006	First Release
1	March 28, 2006	Updated evidence documentation references

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 Multifunction Printer (MFP) Controller Software Version 907.207b. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through December 28, 2004. 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 Multifunction Printer (MFP) Controller Software Version 907.207b Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b Security Target.

1.1.2 Security Target Author

COACT, Inc.

1.1.3 Security Target Publication Date

March 28, 2006

1.1.4 TOE Reference

Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b.

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 2.2.*

1.1.6 Keywords

Multifunction Printer (MFP), Common Criteria (CC), User Authentication, Fax Communications Control, Device Configuration Protection, Touch Screen Lock, 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 MFP Controller Software Version 907.207b Target of Evaluation (TOE). The TOE is the MFP Controller Software Version 907.207b that drives the Lexmark MFP and implements the TOE Security Functions of Fax Communications Control, User Authentication, Device Configuration Protection, and Touch Screen Lock. The TOE resides within the Lexmark MFP.

The Lexmark MFP Printer, Scan Unit with User Interface, Fax modem hardware, and Linux Kernel reside in the IT Environment. They are included by inference and are not part of the TOE. Note that the Linux Kernel does not implement any security functions.

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 Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b 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 Multifunction Printer (MFP) Controller Software Version 907.207b is compliant with the *Common Criteria (CC) for Information Technology Security Evaluation, Version 2.2*, 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 MFP Product Description

B) MFP Controller Software 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. It consists of a printer unit and a scan unit (with an integrated touch-sensitive operator panel) which are connected via a dedicated network connection. The printer is exclusively oriented towards receiving print jobs and producing hardcopy pages, while the scan unit coordinates and controls the use of the scan function, interacts with the user through the integrated touch-panel, and distributes scanned data appropriately.

Figure 1. Lexmark MFP Product Description

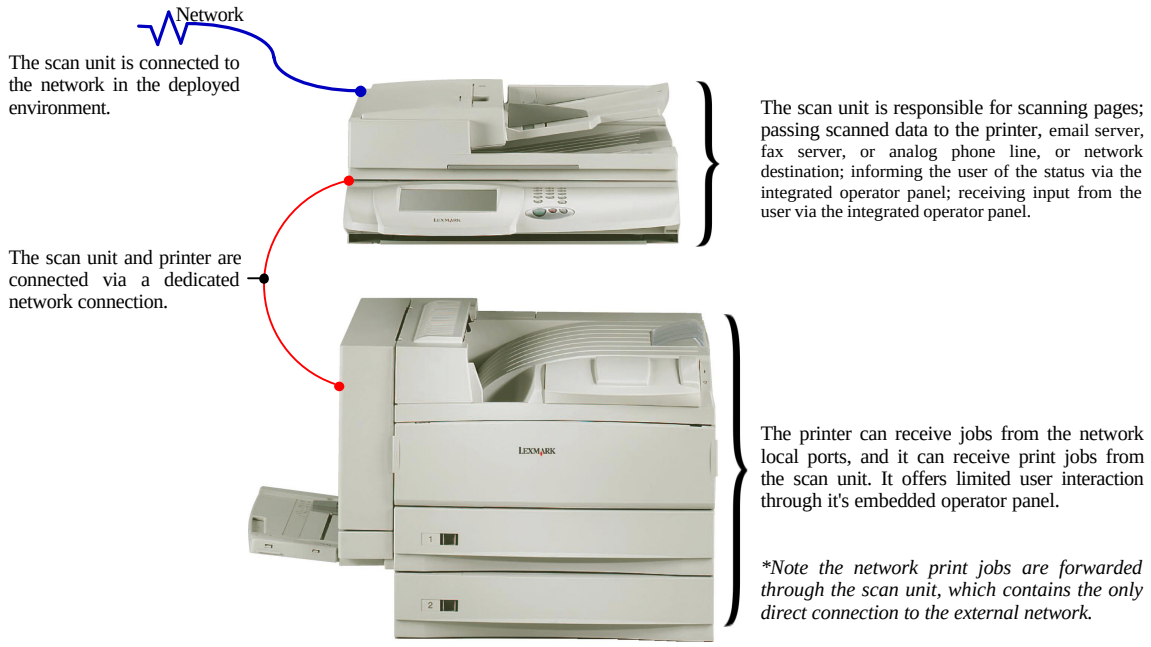


Figure 2. MFP Scanners Showing MFP Controller Locations

The Lexmark MFP includes an array of MFP products that share a common set of functionality. There are eight specific products that share the security functions described in this document: the Lexmark x634e MFP, x634dte MFP, x762e MFP, x820e MFP, x830e MFP, x832e MFP, and x912e MFP. A comparison of the MFP models and their nomenclature is depicted in Table 1.

Table 1. Comparison of MFP Models and Nomenclature

MFP Model	Scan Unit Model	Printer Model
X634e	X4500	T634
X634dte	X4500	T634dt
X762e	X4500	C762
X820e	X7500	W820
X830e	X7500	W820
X832e	X7500	W820
X912e	X5500	C912

Scan units X4500 and X5500 have the same basic architecture in that the MFP is housed in the scan unit. Scan unit X7500 has a “vault” that is external to the scan unit which contains the MFP Controller. All of the scan units have identical touch screen operator panels.

The scan unit handles control for jobs that are initiated through a scan operation (i.e. copying, scan-to-fax, scan-to-email), with the printer primarily acting as the recipient of jobs that require printed pages.

2.2 TOE Description

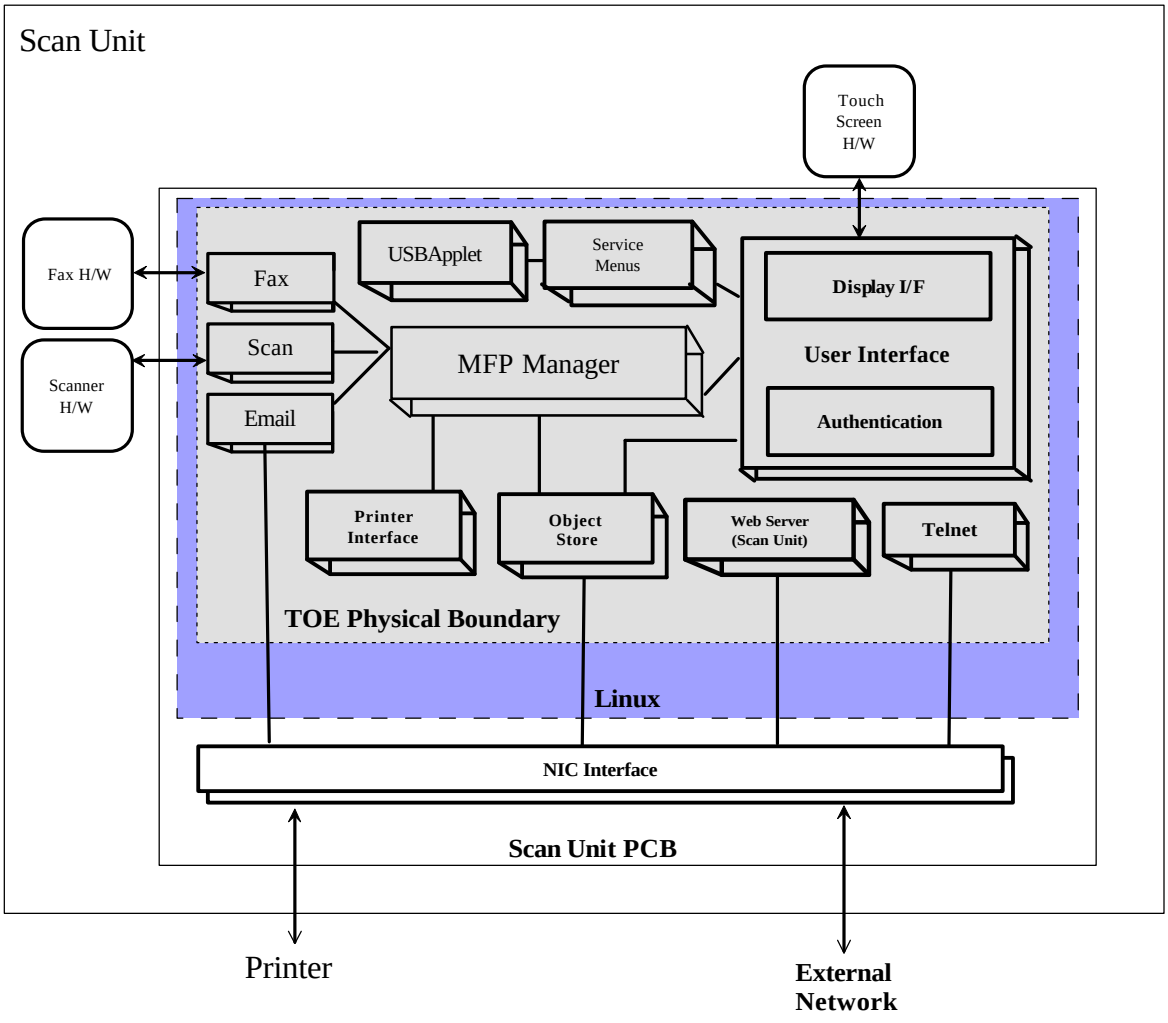
This Security Target defines the requirements for the Lexmark MFP Controller Software Version 907.207b Target of Evaluation (TOE). The TOE is the MFP Controller Software Version 907.207b that drives the Lexmark MFP and implements the TOE Security

Functions of Fax Communications Control, User Authentication, Device Configuration Protection, and Touch Screen Lock. The TOE resides within the Lexmark MFP.

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, as shown in Figure 4 below, consists of the MFP Controller Software Version 907.207b. The TOE consists of application code which is resident on a Printed Circuit Board (PCB) in the Scan Unit. The firmware executes on top of a Linux kernel. Both Linux and the physical PCB are outside the TOE boundary. The grey shaded rectangle in the figure below indicates the TOE physical boundary.

Figure 3. TOE Physical Boundary



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. To ensure this, the TOE maintains control over the transfer of all data during the reception of, or transmission of, a fax job. The fax modem hardware is used to send and receive the data, but control over the data sent remains with the TOE. By restricting the fax modem chip to "Facsimile Class 1" mode, all high-level data transfer operations such as session management and image data handling are performed by the TOE and the fax modem hardware is restricted to performing the low-level exchange of data as directed by the TOE. The TOE ensures that no management or control traffic is exchanged via fax, restricting the traffic to the exchange of image data.

The Fax Communications Control security function is inherent in the design of the system, and is not explicitly activated. The TOE controls incoming fax jobs and treats all incoming data as page facsimile data, which is routed to the MFP's printer component. The data associated with incoming fax jobs is treated exclusively as print data, and there is no mechanism by which telnet, FTP, or other protocols can be routed over the analog fax line.

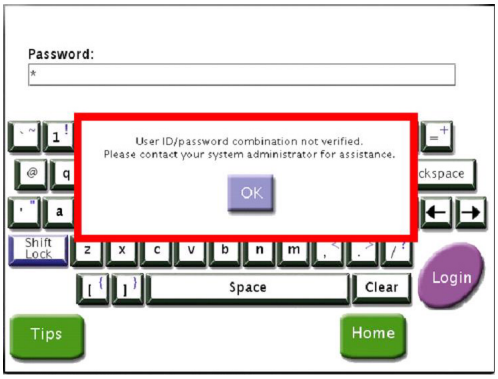
2.4.2 User Authentication

The TOE’s display interface allows access to up to three types of scan-based operations to touch screen users: scan-to-fax, scan-to-copy, and scan-to-email. Each of these operations can be restricted with the User Authentication function. When applied to a type of operation, the User Authentication function 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 from one to fifteen characters in length (per Lexmark administrative guidance, 6 is the minimum)

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.

Figure 4. Three Failed Attempts Notification.



In response to three failed authentication attempts the system does not lock out the **touch screen** user account.

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 associated printer, and have no access to any other security-relevant functions.

2.4.3 Device Configuration Protection

The TOE supports a single system administrator account that has an administrative ID of "MarkNet" This administrative ID cannot be changed. The TOE's administrative password is configurable and is one to eight characters in length (per Lexmark administrative guidance, 6 is the minimum length). The administrative account cannot be deleted, or disabled. There are no means to add any authority to touch screen user accounts.

When using the touch screen operator panel to view or modify device settings, the user is prompted to provide the user name and password for the administrative account. If either an invalid User Name or an invalid Password is specified, access is denied and the user is prompted again. If invalid credentials are provided three times in succession, the user is presented with a notification indicating that access was denied. In response to three failed attempts, the system does not lock out the administrative account.

System Administrators can perform such tasks as creating user accounts, updating user passwords, and changing touch screen lock parameters. 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.

2.4.4 MFP Touch Screen Lock Function

The MFP Touch Screen Lock function allows the MFP's touch screen to be locked, effectively disabling the device's functions such as copy and scan-to-email. This helps to secure the device from unauthorized use at times when the office environment is idle, or

unattended. An administrator must enable the function and set the unlock password for use with the function. When the function is enabled, any user with physical access to the TOE can lock the device's touch screen, and a Touch Screen Unlocker (that knows the password) can unlock the touch screen. The MFP Touch Screen Unlock password mechanism uses a password (alpha and/or numeric digits), not a PIN (numeric digits). The password can be from 1 to 31 characters in length, and is case sensitive (per Lexmark administrative guidance, 6 is the minimum length).

2.4.5 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 software processes, and uses well-defined interfaces for interprocess communication to control interactions between the software processes. Remote login 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 Lexmark MFP Controller Software Version 907.207b Evaluated Configuration

2.5.1 Operational Environment

The evaluated configuration will follow the password instruction as stated in the Lexmark MFP administrative guidance and as detailed below:

A) The minimum password length for the MFP Administrator is six characters.

B) The minimum password length for the MFP Touch Screen Lock is six characters.

C) The minimum password lengths for MFP user accounts are six characters.

D) Internal User Authentication is selected, and applied to all of the user functions accessible via the touch screen operator panel.

E) HTTP is enabled.

F) FTP is disabled.

G) SNMP sets are disabled.

H) The NetWare protocol is disabled.

I) The AppleTalk protocol is disabled.

J) The DLC protocol is disabled.

K) The MVP management protocol is disabled.

L) An external device (e.g., router) must be placed between the scan unit and all users on the network. The external device must be configured to filter all traffic from the users to the scan unit on ports 80 and 10080 (HTTP).

CHAPTER 3

3. TOE Security Environment

This chapter identifies Threats Addressed by the TOE (T), Threats to be Addressed by the Operating Environment (TE), Assumptions (AE), and Organisational Security Policies (P) related to the TOE. Threats are those that are addressed by the TOE and 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 subsections are addressed by the TOE and Operating Environment, respectively.

3.1.1 Threats Addressed by the TOE

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 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 execute TOE security functions without System Administrator privileges.

3.1.2 Threats to be Addressed by the Operating Environment

TE.ACCESS An unauthorized individual may attempt to gain access to information in the MFP not protected by the TOE.

3.2 Assumptions

The assumptions are ordered 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.

3.2.1 Personnel Assumptions

AE.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.

AE.NOEVIL_USER The User is not evil, careless, willfully negligent, nor hostile.

3.2.2 Physical Environment Assumptions

AE.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.

3.2.3 IT Environment Assumptions

AE.ITENV IT Environment is managed and monitored in a secure manner.

AE.NOHTTP The IT Environment shall preclude HTTP communication between network users and the TOE across the IP network to prevent disclosure of the administrator password.

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

O.ACCESS	The TOE identifies and authenticates users prior to allowing access to TOE functions and resources with the exception of Touch Screen Lock function, network print, and fax print operations.
O.ADMINAUTH	The TOE must ensure that the System Administrator is uniquely identified, and that the claimed identity is authenticated, before the System Administrator is granted access to the TOE security management functions.
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.PWDPROTECT	The TOE protects the user, system administrator, and the Touch Screen Lock function 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.
O.TCHSCRNLOCK	The TOE allows any user to lock the touch screen thereby denying walk-up functionality of the TOE.
O.NOTAMPER	The TOE must protect against interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions.

4.2 Security Objectives for the Operating Environment

OE.ACCESS	The IT Environment other than the TOE must protect against unauthorized access to the TOE operating environment.
OE.NOTAMPER	The TOE must be protected against external interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions.
OE.NOHTTP	The IT Environment precludes HTTP communication between network users and the TOE across the IP network.

4.3 Rationale for Security Objectives for the TOE

This section provides the rationale wherein all security objectives are traced back to aspects of the addressed threats.

O.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.ADMINAUTH	O.ADMINAUTH addresses T.NOAUTH and T.ACCESS as it ensures that people attempting to access TOE security management functions are first identified and authenticated.
O.FAX_DESIGN	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.MANAGE	O.MANAGE addresses T.NOAUTH because the TOE provides access by authenticated administrators to those TOE resources and actions for which they have been authorized. The TOE provides the ability to specify and manage user access rights.
O.PWDPROTECT	O.PWDPROTECT addresses T.ACCESS by ensuring that user, system administrator, and Touch Screen Lock function passwords are never viewable in clear text.
O.RESTRICT	O.RESTRICT addresses T.FAXLINE by ensuring that fax operations are separate and distinct from other TOE operations and TOE data.
O.TCHSCRNLOCK	O.TCHSCRNLOCK addresses T.ACCESS by preventing unauthorized users from walking up to the MFP's touch screen and gaining access to the TOE functionality.
O.NOTAMPER	O.NOTAMPER addresses T.ACCESS by ensuring the TOE functions can not be tampered with or bypassed.

Table 2. Mapping Between Security Objectives and Threats for the TOE

	T.FAXLINE	T.ACCESS	T.NOAUTH
O.ACCESS		**X**	
O.ADMINAUTH		**X**	**X**
O.FAX_DESIGN	**X**		
O.MANAGE			**X**
O.PWDPROTECT		**X**	
O.RESTRICT	**X**		
O.TCHSCRLOCK		**X**	
O.NOTAMPER		**X**	

4.4 Rationale for Security Objectives for the Environment

This section provides the rationale wherein all security objectives for the environment are traced back to aspects of the addressed threats or assumptions.

OE.ACCESS	OE.ACCESS addresses TE.ACCESS by ensuring that the operating environment must protect against unauthorized access to information not protected by the TOE in the operating environment, including TOE data stored outside the TOE. OE.ACCESS addresses AE.ITENV by ensuring that the IT Environment is managed and monitored so that unauthorized access to the TOE is prevented. OE.ACCESS addresses AE.NOEVIL because it ensures that the threat from authorized system personnel is low since the operating environment is protected against unauthorized access to TOE information in the operating environment, including TOE data stored outside the TOE. The security functional and assurance provisions employed in the operating environment also ensure reduced risk to the TOE. OE.ACCESS addresses AE.NOEVIL_USER because users are non-evil therefore ensuring that the threat from authorized system personnel is low. OE.ACCESS addresses AE.LOCATE by ensuring that the threat is low from unauthorized physical access by hostile individuals who could compromise the TSF since the operating environment is protected against unauthorized access to TOE information in the operating environment, including TOE data stored outside the TOE.
OE.NOTAMPER	OE.NOTAMPER addresses TE.ACCESS because it ensures that there is no way to disable or bypass the security enforcement functions of the TOE.
OE.NOHTTP	OE.NOHTTP addresses AE.NOHTTP by precluding all HTTP communication between network users and the TOE. HTTP communication does not protect the messages against disclosure and passwords would need to be passed in the clear between the components if HTTP was permitted.

Table 3. Mapping Between Security Objectives, Threats, and Assumptions for the Environment

	TE.ACCESS	AE.NOEVIL	AE.NOEVIL_USER	AE.LOCATE	AE.ITENV	AE.NOHTTP
OE.ACCESS	**X**	**X**	**X**	**X**	**X**	
OE.NOTAMPER	**X**					
OE.NOHTTP						**X**

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 2.2* 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 4. Security Functional Requirements (SFRs)

Security Functional Requirements	
FDP_IFC.1	Subset Information Flow Control
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

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

Table 5. Explicitly Stated Security Functional Requirements

Explicitly Stated Security Functional Requirements	
FDP_IFF.1-NIAP-0407	Simple Security Attributes
FPT_FAX_EXP.1	Fax Communications Control
FPT_LOCK_EXP.1	Touch Screen Lock Function
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs
FPT_SEP_SFT.1	TSF Domain Separation for Software TOEs
FPT_RVM_OS.1	Non-bypassability of the TSP for OSs
FPT_SEP_OS.1	TSF Domain Separation for OSs
FIA_UNLOCK_EXP.1	Touch Screen Lock Function

5.1.1 Class FIA: Identification and Authentication

5.1.1.1 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components

FIA_UAU.1.1 The TSF shall allow *Touch Screen locking, network print, and fax print operations* 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 on the printer associated with the scanner unit.*

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.

Dependencies: FIA_UID.1 Timing of identification

5.1.1.2 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components

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

Dependencies: FIA_UAU.1 Timing of Authentication

5.1.1.3 FIA_UID.1 Timing of Identification

Hierarchical to: No other components

FIA_UID.1.1 The TSF shall allow *Touch Screen locking, network print and fax print operations* on behalf of the user to be performed before the user is identified**.**

Iteration:

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.

Dependencies: No dependencies

Class FMT: Security Management

5.1.1.4 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components

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, and Touch Screen Lock function* to *the System Administrator.*

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

5.1.1.5 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components

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

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

5.1.1.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

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, system administrator, and Touch Screen Unlock passwords; and enabling/disabling the Touch Screen Lock function.*

Dependencies: No dependencies

5.1.1.7 FMT_SMR.1 Security Roles

Hierarchical to: **No other components.**

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

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

Dependencies: FIA_UID.1 Timing of identification

5.1.2 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, Version 2.2.*

5.1.2.1 FPT_FAX_EXP.1 Fax Communications Control

Hierarchical to: No other components

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 and outside 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.

Dependencies: No dependencies

5.1.2.2 FPT_LOCK_EXP.1 Touch Screen Lock Function

Hierarchical to: No other components

FPT_LOCK_EXP.1 The TSF shall allow any user with physical access to the TOE to lock the Touch Screen using the Touch Screen Lock function.

5.1.2.3 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

Hierarchical to: No other components

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

Dependencies: No dependencies

5.1.2.4 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

Hierarchical to: No other components

FPT_SEP_SFT.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

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

Dependencies: No dependencies

5.1.2.5 FIA_UNLOCK_EXP.1 Unlock Touch Screen Function

Hierarchical to: No other components

FIA_UNLOCK_EXP.1 The TSF shall allow only Touch Screen Unlockers to unlock the Touch Screen using the Touch Screen Lock function.

Dependencies: No dependencies

5.2 Security Functional Requirements for the IT Environment

The IT Environment security functional requirements for this Security Target consist of the following components from Part 2 of the CC.

5.2.1 User Data Protection (FDP)

5.2.1.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The **IT Environment** shall enforce the *No HTTP SFP* on:

Subjects: Network Users

Information: IP Datagrams

Operations: Transmission of IP Datagrams.

5.2.1.2 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407 The **IT Environment** shall enforce the *No HTTP SFP* based on the following types of subject and information security attributes:

Network Users: None;

IP Datagrams: Destination IP Address, IP Protocol Identifier, Destination TCP Port.

FDP_IFF.1.2-NIAP-0407 The **IT Environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *If the security attributes of the IP Datagram do not match the criteria of the explicit deny rule, the information flow is permitted.*

FDP_IFF.1.3-NIAP-0407 The **IT Environment** shall enforce the following information flow control rules: *no additional information flow control SFP rules*.

FDP_IFF.1.4-NIAP-0407 The **IT Environment** shall provide the following *no additional SFP capabilities*.

FDP_IFF.1.5-NIAP-0407 The **IT Environment** shall explicitly authorise an information flow based upon the following rules: *no explicit authorisation rules*.

FDP_IFF.1.6-NIAP-0407 The **IT Environment** shall explicitly deny an information flow based upon the following rules:

If all of the following conditions are true:

1. *The IP Destination Address matches the IP Address of the MFP on which the TOE is executing;*
2. *The IP Protocol Identifier is the value for TCP; and*
3. *The TCP Destination Port is either 80 or 10080.*

5.2.2 Protection of the TSF (FPT)

5.2.2.1 5.2.1.1 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs

Hierarchical to: No other components

FPT_RVM_OS.1.1 The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

Dependencies: No dependencies

5.2.2.2 FPT_SEP_OS.1 TSF Domain Separation for OSs

Hierarchical to: No other components

FPT_SEP_OS.1.1 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_OS.1.2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

Dependencies: No dependencies

5.3 Rationale for TOE Security Functional Requirements

This section provides the rationale for the security functional requirements and demonstrates how each security objective is enforced by the security functional requirements.

FIA_UAU.1	FIA_UAU.1 supports O.ACCESS by ensuring that only the Touch Screen Lock function, network print, and fax print can be performed before user authentication.
FIA_UAU.1	FIA_UAU.1 supports O.ADMINAUTH by ensuring that each administrator be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.7	FIA_UAU.7 supports O.PWDPROTECT by ensuring that only obscured feedback is provided to the user when entering passwords.
FIA_UID.1	FIA_UID.1 supports O.ACCESS by ensuring that only the Touch Screen Lock function, network print, and fax print can be performed before the user is identified.
FIA_UID.1	FIA_UID.1 supports O.ADMINAUTH by ensuring that administrators are successfully identified before accessing any other security management functionality of the TOE.
FMT_MOF.1	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	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 FMT_SMF.1 supports O.MANAGE by defining the set of security functions available on the TOE.

FMT_SMR.1 FMT_SMR.1 supports O.MANAGE by ensuring that the security management functions are authorized to the proper roles.

5.4 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 2.2.*

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

Table 6. Explicitly Stated Security Functional Requirements

Explicitly Stated SFR	Rationale
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.
FPT_LOCK_EXP.1	FPT was chosen as the class because the security function involves protection of the TSF. The security function allows any user to lock the Touch Screen without identifying or authenticating.
FPT_RVM_SFT.1	Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE. See FPT_RVM_OS (levied on the IT Environment) for the remaining functionality.
FPT_SEP_SFT.1	Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP_OS (levied on the IT Environment) for the remaining functionality.
FIA_UNLOCK_EXP.1	FIA was chosen as the class because the

Explicitly Stated SFR	Rationale
	security function involves authentication. The security function allows any user trusted with the unlock password to unlock the touch screen.
FPT_RVM_OS.1	Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM_SFT (levied on the TOE) for the remaining functionality.
FPT_SEP_OS.1	Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP_SFT (levied on the TOE) for the remaining functionality.
FDP_IFF.1-NIAP-0407	The ST incorporates all relevant NIAP interpretations as of the start of the evaluation.

FPT_FAX_EXP.1.1 FPT_FAX_EXP.1.1 supports O.FAX_DESIGN and O.RESTRICT by ensuring that the TOE operates only in "Facsimile Class 1" mode forcing the chip to send and receive only fax packets and disallowing the exchange of data packets.

FPT_FAX_EXP.1.2 FPT_FAX_EXP.1.2 supports O.FAX_DESIGN and O.RESTRICT since there is no mechanism by which telnet, FTP, or other protocols can be routed through the fax port thereby mitigating the risk that user data stored in the TOE and outside the TOE will be vulnerable to exploitations via the fax port.

FPT_FAX_EXP.1.3 FPT_FAX_EXP.1.3 supports O.FAX_DESIGN and O.RESTRICT ensuring that the TOE cannot be configured or managed via the fax port since management functionality can only occur through the TOE's web interface or the MFP's touch screen operator panel.

FPT_LOCK_EXP.1 FPT_LOCK_EXP.1 supports O.TCHSCRNLOCK by allowing users to put the MFP (including the TOE) in lock mode using the Touch Screen Lock function. An explicitly

	stated requirement is necessary because there are no standard CC components that specify use of a password without an associated user ID.
FPT_RVM_SFT.1	FPT_RVM_SFT.1 supports O.NOTAMPER by ensuring the TSF cannot be bypassed by actions within the TSC.
FPT_SEP_SFT.1	FPT_SEP_SFT.1 supports O.NOTAMPER by ensuring the TSF cannot be interfered with by subjects within the TSC.
FIA_UNLOCK_EXP.1	FIA_UNLOCK_EXP.1 supports O.ACCESS and O.MANAGE by ensuring that the TSF shall allow only users from the internally stored list, that know the Touch Screen lock/unlock password, to unlock the touch screen. An explicitly stated requirement is necessary because there are no standard CC components that specify use of a password without an associated user ID.
FDP_IFF.1-NIAP-0407	FDP_IFF.1-NIAP-0407 supports OE.NOHTTP by specifying the attributes and rules used to preclude HTTP traffic between network users and the TOE.

The following table contains a mapping of the security functional requirements and the security objectives each requirement enforces.

Table 7. Mapping between Security Functional Requirements and Security Objectives for the TOE

	O.ACCESS	O.ADMINAUTH	O.MANAGE	O.RESTRICT	O.FAX_DESIGN	O.PWDPROTECT	O.TCHSCRLOCK	O.NOTAMPER
FIA_UAU.1	**X**	**X**						
FIA_UAU.7						**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**	**X**			
FPT_LOCK_EXP.1							**X**	

	O.ACCESS	O.ADMINAUTH	O.MANAGE	O.RESTRICT	O.FAX_DESIGN	O.PWDPROTECT	O.TCHSCRLOCK	O.NOTAMPER
FPT_RVM_SFT.1								**X**
FPT_SEP_SFT.1								**X**
FIA_UNLOCK_EXP.1	**X**		**X**					

5.5 Rationale for IT Environment Security Functional Requirements

This section lists the functional requirements levied on the environment and the security objectives satisfied by the environment that each requirement enforces.

FDP_IFC.1 FDP_IFC.1 supports OE.NOHTTP by specifying the subjects, information, and operations involved in precluding HTTP traffic between network users and the TOE.

FDP_IFF.1-NIAP-0407 FDP_IFF.1-NIAP-0407 supports OE.NOHTTP by specifying the attributes and rules used to preclude HTTP traffic between network users and the TOE.

FPT_RVM_OS.1 FPT_RVM_OS.1 supports OE.NOTAMPER since ensuring that TSP enforcement is always invoked before security functions within the TSC are allowed to proceed mitigates the risk that unauthorized modifications of the TOE will occur.

FPT_SEP_OS.1 FPT_SEP_OS.1 supports OE.NOTAMPER since ensuring that the TSF is protected against interference and tampering by untrusted subjects mitigates the risk that unauthorized modifications of the TOE will occur.

The following table contains a mapping of the functional requirements and the security objectives each requirement enforces.

Table 8. Mapping Between IT Environment SFRs and Objectives

	OE.NOTAMPER	OE.NOHTTP
FDP_IFC.1		X
FDP_IFF.1-NIAP-0407		X
FPT_RVM_OS.1	X	
FPT_SEP_OS.1	X	

5.6 Rationale for Security Functional Requirements and Dependencies

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

Table 9. Rationale for Security Functional Requirements and Dependencies

Claim	Hierarchical to	Dependencies
FDP_IFC.1	None	FDP_IFF.1 is satisfied by FDP_IFF.1-NIAP-0407
FDP_IFF.1-NIAP-0407	None	FDP_IFC.1 FMT_MSA.3 is not required because all the security attributes are extracted from each IP datagram as it is processed
FIA_UAU.1	None	FIA_UID.1
FIA_UAU.7	None	FIA_UAU.1
FIA_UID.1	None	None
FMT_MOF.1	None	FMT_SMR.1
FMT_MTD.1	None	FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	None	FIA_UID.1
FPT_FAX_EXP.1	None	None
FPT_LOCK_EXP.1	None	None
FIA_UNLOCK_EXP.1	None	None

FPT_RVM_OS.1	None	None
FPT_SEP_OS.1	None	None

5.7 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 10. 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

5.8 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.

5.9 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, Touch Screen User Authentication Password, and Touch Screen Unlock Password.

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

5.10 Rationale for Strength of Function Claim

5.10.1 MFP Administrative Password

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_UAU.1, FIA_UID.1, and FIA_UNLOCK_EXP.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 six to eight characters in length, and includes both alphabetic characters and non-alphabetic characters.

A password length of six was chosen as the recommended value. One second was used as a conservative length of time required to enter an ID and Password into the Lexmark MFP. 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

= 523486 seconds / 60 seconds

= 8725 minutes / 60 seconds

= 145 hours / 24 hours

= 6.05 days / 365

= 0.017 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’.

5.10.2 MFP Touch Screen Unlock Password

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_UAU.1, FIA_UID.1, and FIA_UNLOCK_EXP.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 Touch Screen Unlock password is one to thirty-one characters in length. The administrator is required to use a minimum password length of 6 according to the guidance documentation. One second is used as a conservative length of time required to enter an ID and Password into the Lexmark MFP. Based on these assumptions, the password space is calculated as follows:

Password length: p = 6

Unique characters: c = 94

Seconds per attempt: s = 1

Average length of successful attack in years =

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

= (1 * 94^6) / (2 * 60 * 60 * 24)

= 689869781056 / 172800

= 3992302 seconds / 60 seconds

= 66538 minutes / 60 minutes

= 1109 hours / 24 hours

= 46.21 days / 365

= 0.1266 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’.

5.10.3 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.

The MFP User Authentication password is password is one to fifteen characters in length. The administrator is required to use a minimum password length of 6 according to the guidance documentation. One second is used as a conservative length of time required to enter an ID and Password into the Lexmark MFP. Based on these assumptions, the password space is calculated as follows:

Password length: p = 6

Unique characters: c = 94

Seconds per attempt: s = 1

Average length of successful attack in years =

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

= (1 * 94^6) / (2 * 60 * 60 * 24)

= 689869781056 / 172800

= 3992302 seconds / 60 seconds

= 66538 minutes / 60 minutes

= 1109 hours / 24 hours

= 46.21 days / 365

= 0.1266 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 *Sections 6.3, 6.4, 6.5* and *Table 11* below.

6.1.1 Fax Communications Control

The Fax Communications Control function assures that the fax function on the MFP is used only to send and receive faxes, i.e. facsimile images of pages. The MFP controls the data that is exchanged via the fax port, and provides no means for a user to establish a fax connection to the MFP, other than to send or receive fax jobs. This means that the user data stored on the MFP, and any data on the network to which the MFP is attached, cannot be accessed via the fax port.

The MFP ensures that all data transferred through the fax connection is related to an incoming or outgoing fax job by maintaining control of the data that is exchanged. The fax hardware that provides the fax connection is kept in "Facsimile Class 1" mode, which restricts the fax hardware such that it does not manipulate or control the exchanged data. By controlling the data exchange directly, and by not implementing any facility for managing the MFP through this connection, and by not supporting any mechanisms such as telnet or FTP over the fax connection, the MFP protects the MFP's data and configuration settings from exploitation via the fax port. The Fax Communications Control function is inherent in the design of the system, and does not need to be explicitly activated by the system administrator or end user.

6.1.2 User Authentication

The MFP’s touch screen interface allows access to up to three types of scan-based operations: scan-to-fax, scan-to-copy, and scan-to-email. Each of these operations can be restricted with the User Authentication function. When applied to a type of operation, the User Authentication function requires the touch screen user’s credentials 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 can be applied to any of the MFP’s scan-based operations, on an individual basis. 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 single system administrator account which has an administrative ID of “MarkNet”. This ID cannot be changed, although the password is configurable. The administrative account cannot be deleted, or disabled. There are no means by which to add any authority to user accounts. System administrators can perform such tasks as creating user accounts, updating user passwords, and changing touch screen lock procedures.

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.

6.1.4 MFP Touch Screen Lock Function

The MFP Touch Screen Lock function allows the MFP's touch screen to be locked, effectively disabling the device's functions: scan-to-fax, scan-to-copy, and scan-to-email. This helps to secure the device from unauthorized use at times when the office environment is idle, or unattended. An administrator must enable the function and set the password for use with the function. Then any user with physical access can lock the device's touch screen, and a Touch Screen Unlocker (that knows the password) can unlock the touch screen. The TOE provides obscured feedback to the Touch Screen Unlocker as the password is entered. This security function contains a permutational mechanism, the Touch Screen Unlock password.

6.1.5 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 11. Assurance Measures and Rationale

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Configuration Management Plan	*Lexmark Configuration Management Practices*, Version 10069-CAP.0.16, dated February 8, 2006 Measures Used to Meet Component: **ACM_CAP.2** 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

Assurance Component	Documentation Satisfying Component	Rationale
		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*, Version 10069-ADO_DEL.0.6, dated December 8, 2005. Measures Used to Meet Component: **ADO_DEL.1** 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*, Version 10069-ADO_DEL.0.6, dated December 8, 2005. Measures Used to Meet Component: **ADO_IGS.1** 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*, Version 10069-FSP.0.18, dated December 21, 2005 Measures Used to Meet Component: **ADV_FSP.1** 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*, Version 10069-HLD.0.10, dated December 21, 2005 Measures Used to Meet Component: **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	Security Target, Functional Specification, and related Design Documentation	*Development Representation Correspondence Document*, Version 10069-RCR.0.5, dated December 8, 2005 Measures Used to Meet Component: **ADV_RCR.1** 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 P/N 16C0591 EC 4G00931*, Version EC4G0093-16C0591.v0.10 Measures Used to Meet Component: **AGD_ADM.1** This requirement is met by the Administration Guidance documentation.

Assurance Component	Documentation Satisfying Component	Rationale
		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 P/N 16C0591 EC 4G00931*, Version EC4G0093-16C0591.v0.10 Measures Used to Meet Component: **AGD_USR.1** 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.
ATE_COV.1	Functional Specification, Test documentation and Test Coverage Analysis.	*Functional Testing of Lexmark Multifunction Printers*, Version 10069.0.7, dated January 6, 2006 Measures Used to Meet Component: **ATE_COV.1** 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.

Assurance Component	Documentation Satisfying Component	Rationale
ATE_FUN.1	Functional Specification, Test documentation and procedures.	*Functional Testing of Lexmark Multifunction Printers*, Version 10069.0.7, dated January 6, 2006 Measures Used to Meet Component: **ATE_FUN.1** 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*, Version 10069.0.7, dated January 6, 2006 Measures Used to Meet Component: **ATE_IND.2** 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 and Developer Vulnerability Analysis Document*, Version 10069-VLA.0.2, Dated December 8, 2005 Measures Used to Meet Component: **AVA_SOF.1** 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	*Strength of Function Analysis and Developer Vulnerability Analysis Document*, Version 10069-VLA.0.2, Dated December 8, 2005 Measures Used to Meet Component: **AVA_VLA.1** This assurance requirement is met by the Vulnerability Analysis, evaluation deliverables and a copy of the TOE suitable

Assurance Component	Documentation Satisfying Component	Rationale
		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.

6.3 Rationale for TOE Security Functions

The following section provides a rationale supporting how the Security Functions satisfy each Security Functional Requirement.

FIA_UAU.1 Timing of Authentication. The User Authentication security function supports FIA_UAU.1 by permitting scan-to-fax, scan-to-copy, and scan-to-email only after user authentication.

FIA_UAU.1 Timing of Authentication. The Device Configuration Protection security function supports FIA_UAU.1 by permitting management access only after administrator authentication.

FIA_UAU.1 Timing of Authentication. The Touch Screen Lock security function supports FIA_UAU.1 by permitting the Touch Screen Lock function before authentication.

FIA_UAU.7 Protected Authentication Feedback. The User Authentication security function supports FIA_UAU.7 by providing obscured feedback to the user while the authentication is in progress.

FIA_UAU.7 Protected Authentication Feedback. The Device Configuration Protection security functions supports FIA_UAU.7 by providing obscured feedback to the administrator while authentication is in progress.

FIA_UAU.7 Protected Authentication Feedback. The MFP Touch Screen Lock security functions supports FIA_UAU.7 by providing obscured feedback to the unlocker while authentication is in progress.

FIA_UID.1 Timing of Identification. The User Authentication security function supports FIA_UID.1 by permitting scan-to-fax, scan-to-copy, and scan-to-email only after user identification.

FIA_UID.1	Timing of Identification. The Device Configuration Protection security function supports FIA_UID.1 by permitting management access only after administrator identification.
FIA_UID.1	Timing of Identification. The Touch Screen Lock security function supports FIA_UID.1 by permitting the Touch Screen Lock function before identification.
FMT_MOF.1	Management of Security Functions Behaviour. The Device Configuration Protection security function supports FMT_MOF.1 by ensuring that only system administrators can access Security Management Functions.
FMT_MTD.1	Management of TSF Data. 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	Specification of Management Functions. 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, system administrator and touch screen unlock passwords; and enabling/disabling the Touch Screen Lock function.
FMT_SMR.1	Security Roles. The Device Configuration Protection function support FMT_SMR.1 by ensuring that TSF management operations are limited to the administrator role

6.4 Rationale for TOE Security Functions versus Explicitly Stated Security Functional Requirements

The following section provides a rationale supporting how the Security Functions satisfy each Explicitly Stated Security Functional Requirement.

FPT_FAX_EXP.1	Fax Communication Control. 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_LOCK_EXP.1	Touch Screen Lock. The Touch Screen Lock security function supports FPT_LOCK_EXP.1 by ensuring that the TSF shall allow any user to lock the touch screen.
FPT_RVM_SFT.1	TSF Self Protection. The TSF Self Protection security function supports FPT_RVM_SFT.1 by ensuring that TSP enforcement is always invoked before security functions within the TSC are allowed to proceed.
FPT_SEP_SFT.1	TSF Self Protection. The TSF Self Protection security function supports FPT_SEP_SFT.1 by ensuring that the

	TSF is protected against interference and tampering by untrusted subjects.
FIA_UNLOCK_EXP.1	Touch Screen Lock. The Touch Screen Lock security function supports FIA_UNLOCK_EXP.1 by ensuring that the TSF shall allow only authorized users to unlock the touch screen.

Table 12. Mapping of Functional Requirements to Security Functions

	Fax Communication Control	User Authentication	Device Configuration Protection	Touch Screen Lock Function	TSF Self Protection
FIA_UAU.1		X	X	X	
FIA_UAU.7		X	X	X	
FIA_UID.1		X	X	X	
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_FAX_EXP.1	X				
FPT_LOCK_EXP.1				X	
FIA_UNLOCK_EXP.1				X	
FPT_RVM_SFT.1					X
FPT_SEP_SFT.1					X

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 Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.3 - 5.6 provide the security functional requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.