Lexmark X466, X656, X658, X738, X860, X862, X864 Multi-Function Printers and InfoPrint 1940, 1870, 1880, Color 1866, 1948, 1968, 1988 Multi-Function Printers Security Target

Version 2.8

October 21, 2010

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

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Lexmark International, Inc.
740 New Circle Road
Lexington, KY 40550
http://www.lexmark.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Lexmark X466 (LR.BR.P311CCa), X656 (LR.MN.P311CCa), X658 (LR.MN.P311CCa), X738 (LR.FL.P311CCa), X860 (LR.SP.P311CCa), X862 (LR.SP.P311CCa) and X864 (LR.SP.P311CCa) Multi-Function Printers and InfoPrint 1940 MT-Model 4570-gh1, gh2, gt1, gt2 (LR.BR.P311CCa), 1870 MT-Model 4567-gh1, gh2, gt1, gt2 (LR.MN.P311CCa), 1880 MT-Model 4568-gs1, gs2, gf1, gf2, gb1, gb2, g11, g12, g21, g22, g31, g32 (LR.MN.P311CCa), Color 1866 MT-Model 4915-gd1, gd2, gt1, gt2 (LR.FL.P311CCa), 1948 MT-Model 4857-g01, g02, g11, g12 (LR.SP.P311CCa), 1968 MT-Model 4858-gt1, gt2, g21, g22 (LR.SP.P311CCa) and 1988 MT-Model 4859-gt1, gt2, g31, g32 (LR.SP.P311CCa) Multi-Function Printers. 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 FIGURES

LIST OF TABLES

ACRONYMS LIST

AES ..... **Advanced Encryption Standard**
AIO ..... **All In One**
BSD ..... **Berkeley Software Distribution**
CAC ..... **Common Access Card**
CC ..... **Common Criteria**
CM ..... **Configuration Management**
EAL ..... **Evaluation Assurance Level**
ESP ..... **Encapsulating Security Payload**
FTP ..... **File Transfer Protocol**
GSSAPI ..... **Generic Security Services Application Program Interface**
HTTP ..... **HyperText Transfer Protocol**
I&A ..... **Identification & Authentication**
IPSec ..... **Internet Protocol Security**
IPv4 ..... **Internet Protocol version 4**
IPv6 ..... **Internet Protocol version 6**
ISO ..... **International Standards Orgaization**
IT ..... **Information Technology**
KDC ..... **Key Distribution Center**
LAN ..... **Local Area Network**
LDAP ..... **Lightweight Directory Access Protocol**
MB ..... **MegaByte**
MFD ..... **Multi-Finction Device**
MFP ..... **Multi-Function Printer**

NTP ..... **Network Time Protocol**
OSP ..... **Organizational Security Policy**
PIV ..... **Personal Identity Verification**
PJL ..... **Printer Job Language**
PKI ..... **Public Key Infrastructure**
PP ..... **Protection Profile**
RFC ..... **Request For Comments**
SASL ..... **Simple Authentication and Security Layer**
SFP ..... **Security Function Policy**
SFR ..... **Security Functional Requirement**
SMTP ..... **Simple Mail Transport Protocol**
ST ..... **Security Target**
TFTP ..... **Trivial File Transfer Protocol**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
UI ..... **User Interface**
URL ..... **Uniform Resource Locator**
USB ..... **Universal Serial Bus**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Lexmark X466 (LR.BR.P311CCa), X656 (LR.MN.P311CCa), X658 (LR.MN.P311CCa), X738 (LR.FL.P311CCa), X860 (LR.SP.P311CCa), X862 (LR.SP.P311CCa) and X864 (LR.SP.P311CCa) Multi-Function Printers and InfoPrint 1940 MT-Model 4570-gh1, gh2, gt1, gt2 (LR.BR.P311CCa), 1870 MT-Model 4567-gh1, gh2, gt1, gt2 (LR.MN.P311CCa), 1880 MT-Model 4568-gs1, gs2, gf1, gf2, gb1, gb2, g11, g12, g21, g22, g31, g32 (LR.MN.P311CCa), Color 1866 MT-Model 4915-gd1, gd2, gt1, gt2 (LR.FL.P311CCa), 1948 MT-Model 4857-g01, g02, g11, g12 (LR.SP.P311CCa), 1968 MT-Model 4858-gt1, gt2, g21, g22 (LR.SP.P311CCa) and 1988 MT-Model 4859-gt1, gt2, g31, g32 (LR.SP.P311CCa) Multi-Function Printers. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*and all international interpretations through August 20, 2009. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Lexmark X466, X656, X658, X738, X860, X862, X864 Multi-Function Printers and InfoPrint 1940, 1870, 1880, Color 1866, 1948, 1968, 1988 Multi-Function Printers Security Target, version 2.8, October 21, 2010.

1.2 TOE Reference

Lexmark X466 (LR.BR.P311CCa), X656 (LR.MN.P311CCa), X658 (LR.MN.P311CCa), X738 (LR.FL.P311CCa), X860 (LR.SP.P311CCa), X862 (LR.SP.P311CCa) and X864 (LR.SP.P311CCa) Multi-Function Printers and InfoPrint 1940 MT-Model 4570-gh1, gh2, gt1, gt2 (LR.BR.P311CCa), 1870 MT-Model 4567-gh1, gh2, gt1, gt2 (LR.MN.P311CCa), 1880 MT-Model 4568-gs1, gs2, gf1, gf2, gb1, gb2, g11, g12, g21, g22, g31, g32 (LR.MN.P311CCa), Color 1866 MT-Model 4915-gd1, gd2, gt1, gt2 (LR.FL.P311CCa), 1948 MT-Model 4857-g01, g02, g11, g12 (LR.SP.P311CCa), 1968 MT-Model 4858-gt1, gt2, g21, g22 (LR.SP.P311CCa) and 1988 MT-Model 4859-gt1, gt2, g31, g32 (LR.SP.P311CCa) Multi-Function Printers

1.3 Evaluation Assurance Level

Assurance claims conform to EAL3 (Evaluation Assurance Level 3) augmented with ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1.

1.4 Keywords

Hardcopy, Paper, Document, Printer, Scanner, Copier, Facsimile, Fax, Document Server, Document Storage and Retrieval, Nonvolatile storage, Residual data, Temporary data, Disk overwrite, Network interface, Shared communications medium, Multifunction Device, Multifunction Product, All-In-One, MFD, MFP

1.5 TOE Overview

1.5.1 Usage and Major Security Features

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

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
2. Administrators authorize Users to use the functions of the TOE.
3. User Document Data are protected from unauthorized disclosure or alteration.
4. User Function Data are protected from unauthorized alteration.
5. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
6. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
7. Document processing and security-relevant system events are recorded, and such records are protected from disclosure or alteration by anyone except for authorized personnel.

1.5.2 TOE type

Miscellaneous (Multifunction Hard Copy Device)

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE is a complete MFP, including the firmware and hardware. To be fully operational, any combination of the following items may be connected to the TOE:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.
2. A telephone line for fax capability.
3. IT systems that submit print jobs to the MFP via the network using standard print protocols.
4. IT systems that send and/or receive faxes via the telephone line.
5. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
6. LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
7. Card reader and cards to support PKI authentication using Common Access Card (CAC) or Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card readers are:
    a. Omnikey 5121 SmartCard Reader,
    b. Omnikey 5321 SmartCard Reader,
    c. Omnikey 5125 SmartCard Reader,
    d. Omnikey 3121 SmartCard Reader,
    e. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),
    f. SCM SCR 331.

1.6 TOE Description

The TOE provides the following functions related to MFPs:

1. Printing – producing a hardcopy document from its electronic form
2. Scanning – producing an electronic document from its hardcopy form
3. Copying – duplicating a hardcopy document
4. Faxing – scanning documents in hardcopy form and transmitting them in electronic form over telephone lines, and receiving documents in electronic form over telephone lines and printing them in hardcopy form

All of the MFPs included in this evaluation provide the same security functionality. Their differences are in the speed and type (color or monochrome) of printing. For the InfoPrint MFPs, a common brand name is used for MFPs both with and without a hard drive. Therefore, the MT-Model is also included in the specification to limit the MFPs in this evaluation to only those including a hard drive. Multiple MT-Models are listed since they distinguish options such as staplers and paper tray sizes. The following tables summarize the technical characteristics of the models.

Table 1 - Technical Characteristics of the Lexmark MFP Models

Model	Color/ Mono	Processor	Pages Per Minute
X466	Mono	500 MHz ARM	40
X656	Mono	600 MHz PowerPC	55
X658	Mono	600 MHz PowerPC	55
X738	Color	900 MHz PowerPC	35
X860	Mono	1 GHz PowerPC	35
X862	Mono	1 GHz PowerPC	45
X864	Mono	1 GHz PowerPC	55

Table 2 - Technical Characteristics of the InfoPrint MFP Models

Brand Nname	MT-Model	Color/ Mono	Processor	Pages Per Minute
1940 MFP	4570-gh1, gh2, gt1, gt2	Mono	500 MHz ARM	40
1870 MFP	4567-gh1, gh2, gt1, gt2	Mono	600 MHz PowerPC	55
1880 MFP	4568-gs1, gs2, gf1, gf2, gb1, gb2, g11, g12, g21, g22, g31, g32	Mono	600 MHz PowerPC	55
Color 1866 MFP	4915-gd1, gd2, gt1, gt2	Color	900 MHz PowerPC	35
1948 MFP	4857-g01, g02, g11, g12	Mono	1 GHz PowerPC	35
1968 MFP	4858-gt1, gt2, g21, g22	Mono	1 GHz PowerPC	45
1988 MFP	4859-gt1, gt2, g31, g32	Mono	1 GHz PowerPC	55

The Target of Evaluation (TOE) is described using the standard Common Criteria terminology of Users, Objects, Operations, and Interfaces. Two additional terms are introduced: Channel describes both data interfaces and hardcopy document input/output mechanisms, and TOE

Owner is a person or organizational entity responsible for protecting TOE assets and establishing related security policies. In this document, the terms User and Subject are used interchangeably.

Figure 1 - TOE Model

The following prefixes are used to indicate different entity types:

Table 3 - Notational prefix conventions

Prefix	Type of entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security Attribute

1.6.1 Users

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrator.

Table 4 - Users

Designation		Definition
U.USER		Any authorized User.
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE. In the remainder of this document, the term "Normal User" is used interchangeably with U.NORMAL. The TOE provides user-level permissions to access specific document processing functions (e.g. print, copy). When it is necessary to distinguish the specific permission, that information is supplied. Otherwise the generic terms identified above are used.
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). In the remainder of this document, the terms "Administrator" and "Authorized Administrator" are used interchangeably with U.ADMINISTRATOR. The TOE provides user-level permissions to access specific management functions. When it is necessary to distinguish the specific permission, that information is supplied. Otherwise the generic terms identified above are used.

1.6.2 Objects (Assets)

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. Objects are equivalent to TOE Assets. There are three categories of Objects: User Data, TSF Data, and Functions.

1.6.2.1 User Data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two types of objects: User Document Data, and User Function Data.

Table 5 - User Data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output. For this TOE, D.DOC includes: 1. User data contained in jobs submitted from the network for printing 2. Scanned data to be printed (copying) 3. Scanned data to be faxed 4. Scanned data to be emailed 5. User data in received faxes
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE. For this TOE, D.FUNC includes: 1. Job information for network print jobs 2. Job information for scanned data to be printed (copying)

Designation	Definition
	3. Job information for scanned data to be faxed 4. Job information for scanned data to be emailed 5. Job information for user data in received faxes

1.6.2.2 TSF Data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two types of objects: TSF Protected Data and TSF Confidential Data.

Table 6 - TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

1.6.2.3 Functions

Functions perform processing, storage, and transmission of data that may be present in the TOE. These functions are described in the following table.

Table 7 - Functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which is or can be shared by other users, such as wired or wireless network media and most radio-frequency wireless media

1.6.3 Operations

Operations are a specific type of action performed by a Subject on an Object. Five types of operations are addressed: those that result in disclosure of information (Read), those that result in alteration of information (Create, Modify, Delete), and those that invoke a function (Execute).

1.6.4 Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE.

Private Medium Interface: mechanism for exchanging information that use (1) wired electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous Users; or, (2) Operator Panel and displays that are part of the TOE. It is an input-output channel. The touch panel and phone line are private medium interfaces.

Shared-medium Interface: mechanism for exchanging information that use wired network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple Users. It is an input-output channel. The standard network interface is a shared-medium interface.

Original Document Handler: mechanism for transferring User Document Data in hardcopy form into the TOE. It is an input channel. The scanner is an original document handler.

Hardcopy Output Handler: mechanism for transferring User Document Data out of the TOE in hardcopy form. It is an output channel. The printer is a hardcopy output handler.

1.7 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.

1.8 Logical Boundary

The TOE supports the security functions documented in the following sections.

1.8.1 Audit Generation

The TOE generates audit event records for security-relevant events and transmits them to a remote IT system using the syslog protocol.

1.8.2 Identification and Authentication

The TOE supports I&A with a per-user selection of internal accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment). PKI authentication may also be specified, in which case all authentication must use PKI. A Backup Password mechanism may also be enabled.

1.8.3 Access Control

Access controls configured for functions (e.g. fax usage) and menu access are enforced by the TOE.

1.8.4 Management

Through the touch panel, authorized administrators may configure access controls and perform other TOE management functions.

1.8.5 Operator Panel Lockout

Authorized users may lock and unlock the touch panel. When the touch panel is locked, print jobs are still accepted but they are queued on the disk drive until the touch panel is unlocked.

1.8.6 Fax Separation

The TOE ensures that only fax traffic is sent or received via the attached phone line. Incoming traffic is processed as fax data only; no management access or other data access is permitted. In the evaluated configuration, the only source for outgoing faxes is the scanner.

1.8.7 Hard Disk Encryption

All use data submitted to the TOE and stored on the hard disk is encrypted to protect its confidentiality in the event the hard drive was to be removed from the TOE.

1.8.8 Disk Wiping

In the evaluated configuration, the TOE automatically overwrites disk blocks used to store user data as soon as the data is no longer required. The mechanism used to perform the overwrite complies with NIST SP800-88, and the DSS "Clearing and Sanitization Matrix" (C&SM) available at http://www.sdisac.com/clearing_and_sanitization_matrix.doc.

1.8.9 Secure Communication

The TOE protects the confidentiality and integrity of all information exchanged over the attached network by using IPSec with ESP for all network communication.

1.8.10 Self Test

During initial start-up, the TOE performs self tests on its hardware components and the integrity of the building blocks and security templates.

1.9 TOE Data

1.9.1 TSF Data

Table 8 - TSF Data

Item	Description	D.CONF	D.PROT
Access Control Authorizations	Access control authorizations specify the restrictions on menus or functions. Items may be configured for no security (accessible to everyone), disabled (not accessible), or restricted by a specified security template.	X	
Account Status	Login status information is associated with all accounts used to authenticate against a building block. For each building block and account, the TOE tracks the number of login failures, time of the earliest login failure, and lock status.	X	
Analog Fax - Cancel Faxes	Specifies whether pending faxes can be canceled by users.		X
Analog Fax - Driver to fax	Specifies whether driver fax jobs are treated as PS jobs and printed or sent as faxes.		X
Analog Fax - Enable Fax Receive	Specifies whether incoming faxes may be received.		X
Analog Fax - Fax Forwarding	Specifies whether fax forwarding of incoming faxes to a destination other than the printer) is enabled.		X
Analog Fax - Holding Faxes	Defines conditions for holding incoming faxes.		X
Date and Time Parameters	Controls whether the time is tracked internally or from a remote NTP server. If an NTP server is used, it specifies the parameters for communication with the server.		X
Disk Encryption	Specifies whether or not files stored on disk are encrypted. This parameter must be set to “Enable” during installation and is not accessible to administrators during operation.		X

Item	Description	D.CONF	D.PROT
Disk Wiping - Automatic Method	Specifies the method used for automatic disk wiping.		X
Disk Wiping - Wiping Mode	Controls the mode used for disk wiping.		X
E-mail images sent as	Specifies whether images forwarded via SMTP are sent as an attachment or FTP'd to a file system and sent as a URL.		X
Enable Audit	Determines if the device records events in the secure audit log and (if enabled) in the remote syslog.		X
Enable Fax Scans	Specifies whether users can create faxes with the device's scanner.		X
Enable FTP/TFTP	Enables FTP/TFTP server on the TOE.		X
Enable HTTP Server	Enables HTTP(S) server on the TOE.		X
Enable Remote Syslog	Determines if the device transmits logged events to a remote server.		X
Fax Mode	Specifies whether the fax function is operating in Analog mode or as a Fax Server (outgoing faxes are forwarded to a fax server via SMTP).		X
Fax Server - Enable Analog Receive	This parameter controls whether incoming faxes are supported when operating in fax server mode		X
Fax Storage Location	Specifies the storage location for faxes. This parameter must be set to "Disk" during installation and is not accessible to administrators during operation.		X
Held Print Job Expiration Timer	Specifies the amount of time a received print job is saved for a user to release before it is automatically deleted.		X
Internal Account Building Blocks	The building blocks specify Internal Accounts as the mechanism to be used for I&A or authorizations and specify memberships.	X	
Internal Account Groups	The set of Internal Account Groups may be used to configure group membership for Internal Accounts and authorizations for access controls using Internal Accounts.	X	
IPSec Settings	The configuration parameters for IPSec that require IPSec with ESP for all network communication (IPv4 and/or IPv6) with certificate validation. These parameters are configured during installation and can't be changed during operation.		X
Internal Accounts Required User Credentials	Specifies whether Internal Accounts use username and password or just username for the I&A process.		X
Job Waiting	Specifies whether a print job may be placed in the Held Jobs queue if the required resources (e.g. paper type) are not currently available, enabling subsequent print jobs to be processed immediately		X

Item	Description	D.CONF	D.PROT
LDAP Certificate Verification	Specifies what verification (if any) should be done on the certificate sent by an LDAP server. Demand specifies that the server certificate is requested; if no certificate is provided or if a bad certificate is provided, the session is terminated immediately. Try indicates the server certificate is requested; if no certificate is provided, the session proceeds normally. If a bad certificate is provided, the session is terminated immediately. Allow indicates the server certificate is requested; if no certificate is provided, the session proceeds normally. If a bad certificate is provided, it will be ignored and the session proceeds normally.		X
LDAP+GSSAPI – Certificate	Specifies whether the default certificate or a specific certificate is required when communicating with an LDAP server.		X
LDAP+GSSAPI – MFP Credentials	Specifies the Username and password to be used when performing LDAP queries.	X	
LDAP+GSSAPI Building Blocks	The building blocks specify LDAP+GSSAPI as the mechanism to be used for I&A or authorizations and specify parameters for retrieving information from an LDAP server (e.g. group names to check, search base, required object names).	X	
LES Applications	Specifies whether enhanced service Java applications may be executed on the TOE. This parameter must be set to "Enable" during installation and is not accessible to administrators during operation.		X
Login Restrictions	Determines how many failed authentications are allowed within the "Failure time frame" value before the offending User Name is prevented from accessing any function protected with the same building block for the duration of the "Lockout time" value. The "Panel Login Timeout" determines how long the operator panel can remain idle on the Home screen before the user is logged off automatically.	X	
Network Port	Defines the parameters required for the TOE to communicate via the standard network port		X
PKI Auth Building Block	The building block specifies PKI as the mechanism to be used for I&A or authorizations and specifies parameters for validating the certificate from the card and retrieving information from Active Directory. This building block is configured during installation. It can't be viewed or modified operationally but can be configured in Security Templates.	X	
Remote Syslog Parameters	Defines the communication to the remote syslog system	X	
Security Reset Jumper	Specifies the behavior of the TOE when a position change of the Security Rest Jumper is detected. No Effect indicates the jumper should be ignored. "No Security" preserves all of the building blocks and templates that a user has defined, but resets each access control to its factory default security level. "Reset to Defaults" deletes all building blocks and templates and resets each access control to its factory default security level.		X

Item	Description	D.CONF	D.PROT
Security Templates	Security Templates are used to configure access controls for restricted functions and menus. Each security template specifies 2 building blocks – one for authentication and one for authorization. The 2 building blocks may be the same. The security template also specifies a set of groups that are authorized to access the associated function or menu.	X	
Simple Kerberos Setup	Defines the KDC Address, KDC Port, and Realm for communication with the KDC. KDC communication is required if the TOE is using the LDAP+GSSAPI mechanism.	X	
SMTP Setup Settings	Define the SMTP server to be used to send email from the TOE		X
SMTP Setup Settings - User-Initiated E-mail	Specifies what credentials (if any) are used to authenticate with an external SMTP server.	X	
Touch Panel Menu Display - FTP	Specifies whether or not the FTP icon should be displayed on the touch panel menu.		X
Touch Panel Menu Display - FTP shortcuts	Specifies whether or not the FTP shortcuts icon should be displayed on the touch panel menu.		X
Touch Panel Menu Display - USB Drive	Specifies whether or not the USB Drive icon should be displayed on the touch panel menu.		X
USB Buffer	Disables all activity via the USB device ports.		X
Use Backup Password	Enables access to the Security Menu via the Backup Password	X	

1.9.2 Authentication Data

All the items described in the following table are D.CONF.

Table 9 - Authentication Data

Item	Description
Backup Password	The Backup Password mechanism allows an administrator to access the Security Menu via the touch panel, regardless of the access controls configured for it.
Internal Account Usernames and Passwords	Internal Accounts are used in conjunction with the Internal Account authentication and authorization mechanism. The username and password for each defined account are used with Internal Account authentication.

1.9.3 Security Attributes

All the items described in the following table are D.CONF.

Table 10 - Security Attributes

Item	Description
Group Memberships	The set of group memberships associated with the current session as the result of successful I&A.
Username	The username specified during a successful I&A interaction.

1.9.4 User Data

All the items described in the following table have both a D.DOC and D.FUNC component.

Table 11 - User Data

Item	Description
Copy Job	Data input to the TOE via the scanner and destined for the printer.
Held Faxes	Data received via the fax interface and held until released by an authorized administrator.
Held Jobs	Data received via the network interface that is destined for the printer and held until released at the touch panel by the submitter.
Incoming Fax Job	Data received via the fax interface and destined for the printer.
Network Print Job	Data received via the network interface and destined for the printer. All network print jobs are held until released.
Scanned Job to be Emailed	Data input to the TOE via the scanner and destined for the SMTP server specified by an authorized administrator.
Scanned Job to be Faxed	Data input to the TOE via the scanner and queued for transmission as a fax via the phone line.

1.10 Evaluated Configuration

The following configuration options apply to the evaluated configuration of the TOE:

1. The TOE includes the single Ethernet interface that is part of the standard configuration of every MFP model. No optional network interfaces are installed.
2. No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.
3. All USB ports on the MFPs that perform document processing functions are disabled. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If PKI authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. If a card reader is installed, the PKI authentication functionality is the only I&A mechanism that can be used.
4. All management functions are performed via the touch screen panel and the HTTP(S) server (for remote management) is disabled. This is done to align the TOE with the P2600 protection profiles currently in development, which require many operations to be performed locally (via the touch screen panel). In addition, this mechanism is preferred over remote management capability because it requires physical access to the TOE, is more resistant to brute force password attacks, and precludes network-based attacks on the management functions.
5. Disk encryption is enabled.
6. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.

7. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged. Certificates presented by remote IT systems are validated.
8. Support for AppleTalk, NetWare (IPX) and LexLink are disabled since these protocols do not provide confidentiality and integrity protection.
9. I&A may use Internal Accounts and/or LDAP+GSSAPI on a per-user basis. The Backup Password mechanism may be enabled at the discretion of the administrators. If PKI authentication is used, all I&A must use the PKI authentication mechanism. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.
10. LDAP+GSSAPI and PKI authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific MFP. Binds to LDAP servers for PKI authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.
11. Internal Accounts require both User ID and password (rather than just User ID).
12. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.
13. Disk wiping functionality is configured for automatic mode with a multi-pass method. This approach is the more secure form of disk wiping and is compliant with NIST SP800-88 and the DSS "Clearing and Sanitization Matrix" (C&SM).
14. User data sent by the MFP in email messages is sent as an attachment (not as a web link).
15. No Java applications are loaded into the MFP by Administrators. These applications are referred to as LES applications in end user documentation. The following LES applications are installed by Lexmark before the TOE is shipped: “PKI Authentication”, “PKI Held Jobs”, and “CAC Smartcard Authentication Token”.
16. No option card for downloadable emulators is installed in the TOE.
17. All fax jobs are stored on disk (rather than NAND) to ensure their contents are wiped upon completion of each job. Incoming faxes are always held until released by an authorized administrator.
18. Some form of credentials (device or user) is required to authenticate to the SMTP server.
19. Fax forwarding is disabled to limit the destinations for incoming faxes to the local printer only.
20. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
21. All administrators must be authorized for all of the document processing functions (print, copy, scan, fax).

22. All network print jobs are held until released. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.
23. Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Internal Accounts and the Backup Password:
    - A minimum of 8 characters
    - At least one lower case letter, one upper case letter, and one non-alphabetic character
    - No dictionary words or permutations of the user name
24. All unnecessary network ports are disabled.

The following table defines the combinations of possible input sources and destinations that are included in the evaluated configuration. In the table, the following meanings are used:

- "May Be Disabled Or Restricted" indicates that the functionality is included in the evaluation but may be disabled or restricted to an authorized set of users at the discretion of an administrator
- "Disabled" indicates the functionality exists within the TOE but is always disabled by an administrator for the evaluated configuration
- "n/a" indicates the functionality does not exist in the TOE

Table 12 - Source-Destination Combinations

Source / Destination	Print Protocols (via the Network Interface)	Scanner	Incoming Fax
Printer	May Be Disabled Or Restricted	May Be Disabled Or Restricted	May Be Disabled Or Restricted
Outgoing Fax	Disabled	May Be Disabled Or Restricted	Disabled
Email (via the Network Interface)	n/a	May Be Disabled Or Restricted	Disabled
FTP (via the Network Interface)	n/a	Disabled	Disabled

1.11 Rationale for Non-Bypassability and Separation

The TOE is a stand-alone system that includes all hardware and software required for operation. The TOE is not a general-purpose platform; rather it is a specialized platform with strictly controlled functionality made available to the users. By limiting the functionality, the TSF is protected from corruption or compromise. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). Multiple simultaneous users are

supported, and the TOE enforces separate domains for each process/user to ensure the appropriate attributes and privileges are associated with each process/user.

Further details on non-bypassability and separation are provided in *Lexmark and InfoPrint MFPs With Hard Drives Security Architecture*.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 2

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Protection Profile Conformance

PP Identification: 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A, version 1.0, dated January 2009

PP Conformance: "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A," "2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A," "2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A," "2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A," "2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A," and "2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A"

This Security Target claims demonstrable conformance to the Security Problem Definition (APE_SPD), Security Objectives (APE_OBJ), Extended Components Definitions (APE_ECD), and the Common Security Functional Requirements (APE_REQ) of the referenced PP.

This TOE performs the functions F.PRT, F.SCN, F.CPY, F.FAX, and F.SMI as defined in the referenced PP and claims demonstrable conformance to the SFR packages defined for each of these functions.

Rationale for PP conformance is provided in chapter 8.

2.3 Security Requirement Package Conformance

Security assurance requirement package conformance: EAL3 augmented by ALC_FLR.2

Security functional requirement package conformance: The SFR packages itemized below from the referenced PP.

1. Common Security Functional Requirements
2. 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
3. 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
4. 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
5. 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
6. 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 13 - Assumptions

A.Type	Description
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.
A.IPSEC	IPSec with ESP is used between the TOE and all remote IT systems with which it communicates over the network using IPv4 and/or IPv6.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the Operational Environment.

Table 14 - Threats

T.Type	TOE Threats
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons

3.4 Organisational Security Policies

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for security objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 15 - Organizational Security Policies for the TOE

Name	Definition
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the input-output interfaces of the TOE, operation of the interfaces will be controlled by the TOE and its operational environment.
P.SOFTWARE.VERIFICATION	To detect unintentional malfunction of the TSF, procedures will exist to self-verify TSF data
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 16 - Security Objectives for the TOE

O.Type	Security Objective
O.AUDIT.LOGGED	The TOE shall create a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.INTERFACE.MANAGED	The TOE shall manage the operation of input-output interfaces in accordance with security policies.
O.I&A	The TOE shall provide functionality to identify and authenticate users whose accounts are defined internal to the TOE.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify TSF data.
O.TIME_STAMP	The TOE will provide reliable time stamps for accountability purposes when internal clocks are configured by an administrator.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 17 - Security Objectives of the Operational Environment

OE.Type	Operational Environment Security Objective
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization, have the training, competence, and time to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.

OE.Type	Operational Environment Security Objective
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be analyzed in order to detect potential security violations, and only by authorized persons
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.I&A	The operational environment shall provide functionality to identify and authenticate users whose accounts are defined external to the TOE.
OE.INTERFACE.MANAGED	The operational environment shall provide protection from unmanaged access to TOE interfaces.
OE.IPSEC	All remote IT system with which the TOE communicates over the network using IPv4 and/or IPv6 shall support IPSec with ESP.
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.TIME_STAMP	The Operational Environment will provide reliable time stamps for accountability purposes when NTP is configured by an administrator.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization, and have the training and competence to follow those policies and procedures.

5. Extended Components Definition

5.1 Extended Security Functional Components

5.1.1 FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be allowed by an administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to:	**No other components**
Dependencies:	**FMT_SMF.1 Specification of Management Functions** **FMT_SMR.1 Security roles**

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

5.2 Extended Security Assurance Components

No extended security assurance requirements are defined.

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

SFR operation completed or partially completed in the PP: Bold

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by letters in parentheses following the component or element (e.g., FAU_ARP.1(A)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 18;** *the additional auditable events specified in Table 18*.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 18: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required) in Table 18;** *the internal event number, ISO 8601 time of the event occurrence, severity, and process*.

Table 18 - Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional Information
SECURE AUDIT TURNED ON/OFF	FAU_GEN.1	n/a	Setting (ON or OFF)

Auditable event	Relevant SFR	Audit level	Additional Information
Job Completed	FDP_ACF.1	Not specified	Job identifier
Job Canceled	FDP_ACF.1	Not specified	Job identifier
Print Job Flushed (because no userid was specified)	FDP_ACF.1	Not specified	None
Expired held job deleted (because it was not released)	FDP_ACF.1	Not specified	Userid specified in the PJL SET USERNAME statement
Authorization Failure	FDP_ACF.1	Not specified	Building block type and name
Successful Authorization	FDP_ACF.1	Not specified	Building block type and name
Authentication Failure	FIA_UAU.1, FIA_UID.1	Basic	Building block type and name, attempted user identity
Successful Authentication	FIA_UAU.1, FIA_UID.1	Basic	Building block type and name
Successful Authentication of Local Admin	FIA_UAU.1, FIA_UID.1	Basic	None
Authorization Failure	FMT_MTD.1	Not specified	Building block type and name
Successful Authorization	FMT_MTD.1	Not specified	Building block type and name
Setting change	FMT_MTD.1	Basic	Parameter identifier and new value
Authentication/Authorization Setting CREATION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting CREATION (Success)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting DELETION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting DELETION (Success)	FMT_MTD.1	Basic	Building block type and name
Authentication/Authorization Setting MODIFICATION (FAILURE!)	FMT_MTD.1	Basic	Building block type and name
Authorization Setting MODIFICATION (Success)	FMT_MTD.1	Basic	Building block type and name
Use of the management functions	FMT_SMF.1	Minimum	None
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None
Time changed	FPT_STM.1	Minimum	None
Time change greater than maximum tolerance	FPT_STM.1	Minimum	None
Time changed due to time source change	FPT_STM.1	Minimum	None
Time changed due to Battery Failure	FPT_STM.1	Minimum	None
User logged out due to timeout	FTA_SSL.3	Minimum	None
Failure of the trusted channel	FTP_ITC.1	Minimum	None

Application Note: The audit for "Use of the management functions" is addressed by the "Setting change" and "Authentication/Authorization Setting" audits. It is included in the audit table above for conformance with the P2600 PP.

Application Note: The audit for "Modifications to the group of users that are part of a role" is addressed by the "Authentication/Authorization Setting" audits. It is included in the audit table above for conformance with the P2600 PP.

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1(A) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *random number generator* and specified cryptographic key sizes *256 bits* that meet the following: *X9.31 A.2.4 (AES) (vendor affirmed)*.

Application Note: This instance of the SFR applies to the AES key used for hard disk encryption.

FCS_CKM.1.1(B) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *2048 bits* that meet the following: *PKCS #1 (vendor affirmed)*.

Application Note: This instance of the SFR applies to the RSA public-private key pair generated for the default certificate.

6.1.2.2 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 (vendor affirmed)*.

6.1.2.3 FCS_COP.1 Cryptographic Operation

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

Table 19 - Cryptographic Operations

Algorithm	Operations	Key Size in Bits	Standards
DES (CBC mode)	Encryption, decryption	56	FIPS 46-3
Triple-DES (EDE in CBC mode)		168	FIPS 46-3
AES (CBC mode)		128, 256	FIPS 197
SHA	Hashing	160, 256	FIPS 180-2
MD5		128	RFC 1321
HMAC	Message authentication coding	128, 160	FIPS 198
RSA	Digital signatures	1024, 2048	PKCS#1
Diffie-Hellman	Key agreement	Group 1 (768), Group 2 (1024), Group 14 (2048)	PKCS #3
PRNG	Random number generation	n/a	ANSI X9.31

Application Note: Conformance to the referenced standards is by vendor affirmation.

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1(A) The TSF shall enforce the *Common Access Control SFP* on

1. *Subjects: Users (U.USER)*
2. *Objects: Copy Job, Incoming Fax Job, Network Print Job, Scanned Job to be Emailed, Scanned Job to be Faxed*
3. *Operations: Create, View, Modify, Release, Delete*

Application Note: "Release" refers to releasing held faxes or held jobs to be printed (at which time they can be read). "View" refers the ability to see that the job exists (D.FUNC), not to view the user data inside the job. No functionality exists to view the user data inside a job other than printing the document. "Modify" refers to the ability to change job parameters (e.g. number of copies).

FDP_ACC.1.1(B) The TSF shall enforce the *TOE Function Access Control SFP* on

1. *Subjects: Users (U.USER)*
2. *Objects: TOE Functions - F.PRT, F.SCN, F.CPY, F.FAX, F.SMI*
3. *Operations: Invoke*

FDP_ACC.1.1(C) The TSF shall enforce the *Touch Panel Access Control SFP* on

1. *Subjects: Users (U.USER)*
2. *Objects: Touch Panel*
3. *Operations: Lock, Unlock, Use*

6.1.3.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1(A) The TSF shall enforce the *Common Access Control SFP* to objects based on the following:

1. *Subjects: Users (U.USER) – Username, Group memberships*
2. *Objects: Copy Job, Incoming Fax Job, Network Print Job, Scanned Job to be Emailed, Scanned Job to be Faxed - owner*

FDP_ACF.1.2(A) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the rules specified in the following table*.

Table 20 - Common Access Control SFP Rules

Operation Object	Create	View	Modify	Release	Delete
Copy Job	Allowed if the user is a member of an authorized group of the security template configured for the Copy Function access control. The job owner is the authenticated user of the touch panel.	Allowed for jobs owned by the user	Not allowed	n/a	Allowed for jobs owned by the user
Incoming Fax Job	Allowed if the Fax Function access control is not "disabled", and if the "Enable Fax Receive" or "Enable Analog Receive" parameter is "On". Note that all incoming faxes are held in the evaluated configuration. Incoming faxes are owned by any user that is a member of an authorized group of the security template configured for the Release Held Faxes access control.	Allowed if the user is a member of an authorized group of the security template configured for the Release Held Faxes access control	Not allowed	Allowed if the user is a member of an authorized group of the security template configured for the Release Held Faxes access control	Allowed if the user is a member of an authorized group of the security template configured for the Release Held Faxes access control
Network Print Job	Allowed if the submitted job includes a userid in a SET USERNAME PJL statement and the user is a member of an authorized group for the Solution 1 access control. Note that all incoming network print jobs are held in the evaluated configuration. The job owner is the userid specified in the PJL SET USERNAME statement..	Allowed for jobs owned by the user	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Held Jobs Access access control	Allowed for jobs owned by the user if the user is a member of an authorized group of the security template configured for the Held Jobs Access access control	Allowed for jobs owned by the user
Scanned Job to be Emailed	Allowed if the user is a member of an authorized group of the security template configured for the Fax Function access control; the "Enable Fax Scans" parameter is On; and the "Fax Mode"	Allowed for jobs owned by the user	Not Allowed	n/a	Allowed for jobs owned by the user

Operation Object	Create	View	Modify	Release	Delete
	parameter is “Fax Server”. The job owner is the authenticated user of the touch panel.				
Scanned Job to be Faxed	Allowed if the user is a member of an authorized group of the security template configured for the Fax Function access control; the “Enable Fax Scans” parameter is On; and the “Fax Mode” parameter is “Analog Fax”. The job owner is the authenticated user of the touch panel.	Allowed for jobs owned by the user	Not Allowed	n/a	Allowed for jobs owned by the user

FDP_ACF.1.3(A) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no rules that explicitly authorise access*.

FDP_ACF.1.4(A) The TSF shall explicitly deny access of subjects to objects based on the following rules: *if a listed access control is “Disabled” access is denied*.

FDP_ACF.1.1(B) The TSF shall enforce the *TOE Function Access Control SFP* to objects based on the following:

1. *Subjects: Users (U.USER) – Group memberships*
2. *Objects: TOE Functions (F.PRT, F.SCN, F.CPY, F.FAX, F.SMI) - None*

FDP_ACF.1.2(B) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **the user is explicitly authorized by U.ADMINISTRATOR to use a function**.

FDP_ACF.1.3(B) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no rules that explicitly authorise access*.

FDP_ACF.1.4(B) The TSF shall explicitly deny access of subjects to objects based on the following rules: *if a listed access control is “Disabled” access is denied.*

FDP_ACF.1.1(C) The TSF shall enforce the *Touch Panel Access Control SFP* to objects based on the following:

1. *Subjects: Users (U.USER) – Group memberships*
2. *Objects: Touch Panel - None*

FDP_ACF.1.2(C) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *Lock – A user may lock the Touch Panel if the Operator Panel Lock access control is restricted and that user is a member of an authorized group.*
2. *Unlock – A user may unlock the Touch Panel if the Operator Panel Lock access control is restricted and that user is a member of an authorized group.*
3. *Use – Any user may use the Touch Panel when it is not locked.*

FDP_ACF.1.3(C) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no rules that explicitly authorise access*.

FDP_ACF.1.4(C) The TSF shall explicitly deny access of subjects to objects based on the following rules: *no rules that explicitly deny access.*

6.1.3.3 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: **D.DOC**.

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *the range of 1 to 10* unsuccessful authentication attempts occur related to *accounts within the administratively configured failure time frame.*

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *disable the account for the administratively configured lockout time*.

6.1.4.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. *Username*
2. *Password*
3. *Associated groups*
4. *User permissions, as specified by associated groups and security template configurations*
5. *Number of consecutive authentication failures*
6. *Time of the earliest authentication failure (since the last successful login if any have occurred)*
7. *Account lock status*

6.1.4.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *submission of network print jobs, incoming faxes (if enabled), and usage of the touch panel with menus that have been configured for "no security"* on behalf of the user to be performed before the user is authenticated.

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

Application Note: The TOE only performs the authentication for users using Internal Accounts or the Backup Password. When I&A uses LDAP+GSSAPI or PKI, authentication is under the control of the LDAP server (and CAC/PIV) in the operational environment. For all mechanisms, the TOE restricts access to other functionality until authentication is successful.

6.1.4.4 FIA_UAU.7 Protected Authentication Feedback

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

6.1.4.5 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *incoming faxes (if enabled) and usage of the touch panel with menus that have been configured for "no security"* 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: The TOE only performs the identification for users using Internal Accounts or the Backup Password. When I&A uses LDAP+GSSAPI or PKI, identification is under the control of the LDAP server (and CAC/PIV) in the operational environment. For all mechanisms, the TOE restricts access to other functionality until identification is successful.

6.1.4.6 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

1. *Username*
2. *Password*
3. *Associated groups (for Internal Accounts only)*
4. *User permissions*
5. *Building block name used during authentication*

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

1. *The username and password are the values supplied by the user.*
2. *The associated groups are the values configured for the user account.*
3. *User permissions are determined by the security templates that include groups in the authorization building blocks that are associated groups of the user.*
4. *The building block name is specified in the security template of the item with access control restrictions that required I&A.*

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

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions *listed in the following table* to *administrators that pass the access control check for the authorization item specified for the listed functions*.

Table 21 - Management of Security Functions Behaviour

Function	Authorization Item	Operations
Audit Generation	Security Menus at the device	Disable, enable
Identification & Authentication	Security Menus at the device	Determine the behaviour of, disable, enable, modify the behaviour of
Access Control	Security Menus at the device	Determine the behaviour of, disable, enable, modify the behaviour of
Management	Security Menus at the device	Disable, enable
Operator Panel Lock	Security Menus at the device	Disable, enable
Fax Separation	Security Menus at the device	Disable, enable
	Settings Menu at the device	Determine the behaviour of, modify the behaviour of
Disk Wiping	Security Menus at the device	Determine the behaviour of, disable, enable, modify the behaviour of
Secure Communication	None (IPSec is configured during installation and can't be changed during operation)	None

6.1.5.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *Common Access Control SFP, TOE Function Access Control SFP and Touch Panel Access Control SFP* to restrict the ability to query, modify, delete, *create* the security attributes *Username, associated groups and user permissions* to *administrators authorized for access to the Security Menu*.

6.1.5.3 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *Common Access Control SFP, TOE Function Access Control SFP and Touch Panel Access Control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

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

6.1.5.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create* the *data identified in the following table* to **the authorized identified roles except U.NORMAL**.

Application Note: The user permission for each TSF data item to determine "authorized identified roles" is identified in the following table.

Table 22 - TSF Data

Item	Authorization Menu Item	Operations
Access Control Authorizations	Security Menu at the device	Query, Modify
Analog Fax - Cancel Faxes	Settings Menu at the device	Query, Modify
Analog Fax - Driver to fax	Settings Menu at the device	Query, Modify
Analog Fax - Enable Fax Receive	Settings Menu at the device	Query, Modify
Analog Fax - Enable Manual Fax	Settings Menu at the device	Query, Modify
Analog Fax - Fax Forwarding	Settings Menu at the device	Query, Modify
Analog Fax - Holding Faxes	Settings Menu at the device	Query, Modify, Delete, Create
Backup Password	Security Menu at the device	Modify, Delete, Create
Date and Time Parameters	Security Menu at the device	Query, Modify
Disk Wiping - Automatic Method	Security Menu at the device	Query, Modify
Disk Wiping - Wiping Mode	Security Menu at the device	Query, Modify
Download Target	Settings Menu at the device	Query, Modify
E-mail images sent as	Settings Menu at the device	Query, Modify
Enable Audit	Security Menu at the device	Query, Modify
Enable Fax Scans	Settings Menu at the device	Query, Modify
Enable FTP/TFTP	Network/Ports Menu at the device	Query, Modify
Enable HTTP Server	Network/Ports Menu at the device	Query, Modify
Enable Remote Syslog	Security Menu at the device	Query, Modify
Fax Mode	Settings Menu at the device	Query, Modify
Fax Server - Enable Analog Receive	Settings Menu at the device	Query, Modify
Held Print Job Expiration Timer	Security Menu at the device	Query, Modify
Internal Account Building Blocks	Security Menu at the device	Query, Modify, Delete, Create
Internal Account Groups	Security Menu at the device	Query, Modify, Delete, Create
Internal Account Usernames and Passwords	Security Menu at the device	Query, Modify, Delete, Create
Internal Accounts Required User Credentials	Security Menu at the device	Query, Modify
Job Waiting	Settings Menu at the device	Query, Modify
LDAP Certificate Verification	Security Menu at the device	Query, Modify
LDAP+GSSAPI – Certificate	Security Menu at the device	Query, Modify
LDAP+GSSAPI – MFP Credentials	Security Menu at the device	Query, Modify
LDAP+GSSAPI Building Blocks	Security Menu at the device	Query, Modify, Delete, Create

Item	Authorization Menu Item	Operations
Login Restrictions	Security Menu at the device	Query, Modify
Network Port	Network/Ports Menu at the device	Query, Modify
Remote Syslog Parameters	Security Menu at the device	Query, Modify
Security Reset Jumper	Security Menu at the device	Query, Modify
Security Templates	Security Menu at the device	Query, Modify, Delete, Create
Simple Kerberos Setup	Settings Menu at the device	Query, Modify
SMTP Setup Settings	Network/Ports Menu at the device	Query, Modify
SMTP Setup Settings - User-Initiated E-mail	Network/Ports Menu at the device	Query, Modify
Touch Panel Menu Display - FTP	Settings Menu at the device	Query, Modify
Touch Panel Menu Display - FTP shortcuts	Settings Menu at the device	Query, Modify
Touch Panel Menu Display - USB Drive	Settings Menu at the device	Query, Modify
USB Buffer	Network/Ports Menu at the device	Query, Modify
Use Backup Password	Security Menu at the device	Query, Modify

6.1.5.5 FMT_SMF.1 Specification of Management Functions

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

1. *User management*
2. *Access control management*
3. *Time management*

6.1.5.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *defined by the security-relevant permissions in the following table that can be configured in an operational TOE for users via building blocks in security templates for the specific permissions.*

Table 23 - FMT_SMR.1 Detail

Item	Description	Administrators Only?
Copy Function	Control's a user's access to the Copy functionality	No
E-mail Function	Control's a user's access to the Email functionality (scan to email)	No
Fax Function	Control's a user's ability to perform a scan to fax job When "Disabled", all analog faxing (scan send, receive, and driver send) and the fax server are disabled. The fax icon is removed and the device does not answer incoming calls nor print driver faxes. However, the panel menus still display fax-related settings as though fax were enabled. When protected by a security template, the values of	No

Item	Description	Administrators Only?
	the "Enable Fax Scan", "Driver to Fax", and "Enable Fax Receive" settings in the "Fax Settings Menu" determine the behavior of Fax Receive and Driver Fax. Fax Scan sending is enabled if the user provides valid credentials.	
Network/Ports Menu at the device (and submenus)	Controls access to the Network/ Ports Menu via the Administration Menus	Yes
Operator Panel Lock	Controls access to the "Lock Device" and "Unlock Device" buttons	Yes
Release Held Faxes	Controls access to the Held Faxes button and the Release Held Faxes button on the Home screen	Yes
Reports Menu at the device (and submenus)	Controls access to the Reports Menu via the Administration Menus. This includes information about user jobs, which can't be disclosed to non-administrators.	Yes
Security Menu at the device (and submenus)	Controls access to the Security Menu via the Administration Menus	Yes
Service Engineer Menus at the device (and submenus)	Controls access to any SE menu accessible from the panel, including the Network SE menu	Yes
Settings Menu at the device (and submenus)	Controls access to the Settings Menu via the Administration Menus	Yes
Solution 1	In the evaluated configuration, controls which users are permitted to submit network print jobs and access the Held Jobs menu.	No

Application Note: If any permission identified as "Administrators Only" in the table above is associated with a user account, then that user account is implicitly an Administrator (U.ADMINISTRATOR). If no permission identified as "Administrators Only" in the table above is associated with a user account but any permission not identified as "Administrator Only" is, then that user account is implicitly a Normal User (U.NORMAL). The role "Nobody" applies to a defined user that has no permissions identified in the table above.

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface**.

Application Note: For this TOE, the network interface is the only shared-medium interface.

6.1.6.2 FPT_STM.1 Reliable Time Stamps

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

Application Note: This SFR only applies when the TOE is configured to use internal timestamps. If the TOE is configured to obtain timestamps from an external NTP server, this functionality is provided by that external NTP server in the operational environment.

6.1.6.3 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of *the hardware components of the TSF*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *the security templates and building blocks*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a *period of time configured by an authorized administrator for touch panel sessions.*

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF, the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

Application Note: For this TOE, the network interface is the only shared-medium interface. The TSF requires all IP datagrams entering or leaving the box to use IPSec with ESP (other than the ISAKMP/IKE datagrams used to set up the security associations). If an incoming IP datagram does not satisfy this rule, the TSF attempts to establish a security association with the remote IT system that originated the datagram.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3 augmented by ALC_FLR.2. These requirements are summarized in the following table.

Table 24 - EAL3+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security

Assurance Class	Component ID	Component Title
		measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 25 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	Satisfied Satisfied
FCS_CKM.4	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1]	Satisfied
FCS_COP.1	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	Satisfied Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied Satisfied
FDP_RIP.1	No other components.	None	n/a
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied

SFR	Hierarchical To	Dependency	Rationale
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_FDI_EXP.1	No other components.	FMT_SMR.1	Satisfied
FPT_STM.1	No other components.	None	n/a
FPT_TST.1	No other components.	None	n/a
FTA_SSL.3	No other components.	None	n/a
FTP_ITC.1	No other components.	None	n/a

7. TOE Summary Specification

7.1 Security Functions

7.1.1 Audit Generation

The TOE generates audit event records for security-relevant events. A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated.

Each record format follows the syslog format defined in the Berkeley Software Distribution (BSD) Syslog Protocol (RFC 3164). The TOE supplies the PRI, HEADER, MSG/TAG, and MSG/CONTENT fields for all messages. The CONTENT portion may contain the following fields (in order, separated by commas):

- Event Number
- ISO 8601 time ([YYYY-MM-DD]T[hh:mm:ss])
- Severity
- Process (same as TAG)
- Remote IPv4 address
- Remote IPv6 address
- Remote Hostname
- Remote Port
- Local Port
- Authentication/Authorization method
- Username
- Setting ID
- Setting's new value
- Event name
- Event data

The time field is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured.

Fields in the CONTENT section that are not relevant for specific events are blank. The remote IPv4 address, remote IPv6 address, remote hostname, remote port, and local port fields are always blank for events resulting from actions at the MFP (e.g. usage of the touch panel). The events that cause audit records to be generated are specified in section 6.1.1.1 .

As audit event records are generated, they are forwarded to the remote syslog IT system configured by an administrator.

7.1.2 Identification and Authentication

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

The I&A process is controlled by security templates that are associated with functions and menus. Each security template specifies two building blocks – one for authentication and the second for authorization. The security template also includes a list of groups that are authorized to perform the function or access the menu that the security template is associated with.

When I&A is necessary, the TOE examines the authentication building block in the security template to determine what authentication mechanism should be used. The general purpose mechanisms supported in the evaluated configuration are PKI authentication, Internal Accounts and LDAP+GSSAPI.

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

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

For Internal Accounts and LDAP+GSSAPI , the TOE presents a username entry screen on the touch panel and collects a username, then presents a password entry screen and collects a password. When the password is entered, only asterisks ("*") are displayed. Once the username and password are collected, the next step in the process depends on the I&A mechanism being used.

For Internal Accounts, the TOE performs the validation of the username and password against the set of configured Internal Accounts.

For LDAP+GSSAPI, the TOE forwards the username and password to the configured LDAP server for validation and waits for the response. If no response is received, the validation is considered to have failed.

For Internal Accounts and LDAP+GSSAPI, if the validation fails because of an invalid password (for a valid username), the count of failed authentication attempts is incremented for that building block and account combination. If the threshold for failed attempts within a time period is reached, then the account is marked as being locked for the configured amount of time to mitigate against brute force password attacks. This information is tracked in memory and is not maintained across a restart of the TOE. Note that for LDAP+GSSAPI validations, the server

may also be enforcing limits on authentication failures. These mechanisms operate independently and are not required to be comparably configured.

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

If validation is successful, the TOE binds the username, password, account name, email address, group memberships (for Internal Accounts only) and name of the building block used for authentication to the user session for future use (only the username and group memberships are security attributes). An audit record for the successful authentication is generated.

The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for actions on the Home screen of the touch panel expires. If the inactivity timer expires, an audit record is generated.

If a user locks the touch panel, the user session is terminated immediately. Similarly, after a user unlocks the touch panel, the user session is terminated immediately.

7.1.2.1 Backup Password

The Backup Password mechanism allows an administrator to access the Security Menu via the touch panel, regardless of the access controls configured for it. When a user attempts to access the Security Menu, the authentication prompt displays a "soft" button that enables a user to authenticate with the Backup Password instead of the method that normally secures this menu. This function may be necessary under unusual circumstances, such as when communication with the LDAP server is not operational.

If the correct Backup Password is supplied, the administrator is considered to be successfully authenticated and authorized for access to the Security Menu (only). A "Successful Authentication of Local Admin" audit record is generated. If an incorrect Backup Password is supplied, an error message is displayed on the touch panel, an audit record is generated, and then the display is returned to the previous screen.

If an invalid password is supplied, the count of failed authentication attempts for the Backup Password is incremented. If the threshold for failed attempts within a time period is reached, then the Backup Password is marked as being locked for the configured amount of time to mitigate against brute force password attacks. This information is tracked in memory and is not maintained across a restart of the TOE.

The Backup Password mechanism may be disabled by an authorized administrator via the menus on the touch panel.

7.1.3 Access Control

Access control validates the user access request against the authorizations configured by administrators for specific functions. On a per-item basis, authorization may be configured as "disabled" (no access), "no security" (open to all users), or restricted (via security templates) (some items do not support all three options). Authorization may be configured for the following items:

Table 26 - Access Control Items

Item	Description	Comment
Address Book	Controls access to the Search Address Book button that appears as part of the E-mail, FTP, and Fax functions that are available from the panel's Home screen	Any authorization option may be configured
Cancel Jobs at the device	Controls access to the functionality to cancel jobs via the front panel.	Access must be restricted to authorized users in the evaluated configuration
Change Language	Controls access to the Change Language button on the Home screen (when displayed); this button is NOT displayed by default but a user can activate it via the "General Settings Menu"	Any authorization option may be configured
Color Dropout	Controls a user's ability to activate the Color Dropout functionality as part of a job; if protected and the user fails to authenticate, then the device DOES NOT use the color dropout functionality in the job	Any authorization option may be configured
Configuration Menu (and submenus)	Controls access to the Configuration Menu via the front panel	Must be disabled in the evaluated configuration
Copy Color Printing	Controls a user's ability to copy content in color	Any authorization option may be configured
Copy Function	Control's a user's access to the Copy functionality	Access must be disabled or restricted to authorized users in the evaluated configuration
Create Bookmarks at the device	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen; unless disabled, all users (regardless of their credentials) can search and print bookmarks	Must be disabled in the evaluated configuration
Create Bookmarks Remotely	Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen; unless disabled, all users (regardless of their credentials) can search and print bookmarks	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Create Profiles	Controls the ability to create scan profiles from remote systems.	Must be disabled in the evaluated configuration
E-mail Function	Control's a user's access to the Email functionality (scan to email)	Access must be disabled or restricted to authorized users in the evaluated configuration
eSF Configuration	Controls access to the Embedded Solutions link (and all sublinks) via the Web page	This function is not pertinent to the evaluated configuration since web access is disabled. Therefore, any option may be configured
Fax Function	Control's a user's ability to perform a scan to fax job When "Disabled", all analog faxing	Access must be disabled or restricted to authorized users in the evaluated configuration

Item	Description	Comment
	(scan send, receive, and driver send) and the fax server are disabled. The fax icon is removed and the device does not answer incoming calls nor print driver faxes. However, the panel menus still display fax-related settings as though fax were enabled. When protected by a security template, the values of the "Enable Fax Scan", "Driver to Fax", and "Enable Fax Receive" settings in the "Fax Settings Menu" determine the behavior of Fax Receive and Driver Fax. Fax Scan sending is enabled if the user provides valid credentials.	
Firmware Updates	Controls a user's ability to update the device's firmware code via the network	Must be disabled in the evaluated configuration
FTP Function	Controls a user's ability to access the FTP button on the Home Screen (when displayed); the FTP button is hidden by default and does not display unless a user activates it via the Home Screen Customization menu in the "General Settings Menu"	Must be disabled in the evaluated configuration
Held Jobs Access	Controls access to the Held jobs menu if the "PKI Held Jobs" LES application is not installed	Must be disabled in the evaluated configuration
Manage Shortcuts at the device	Controls access to the Manage Shortcuts Menu via the Administration Menus	Access may be configured as restricted or no security, but not disabled
Manage Shortcuts Remotely	Controls access to the Manage Shortcuts Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Network/Ports Menu at the device (and submenus)	Controls access to the Network/ Ports Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Network/Ports Menu Remotely	Controls access to the Network/ Ports Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
NPA Network Adapter Setting Changes	When "Disabled", prohibits any changes to the network system adapter via NPA commands	Must be disabled in the evaluated configuration
Operator Panel Lock	Controls access to the "Lock Device" and "Unlock Device" buttons	Access may be configured as restricted or disabled
Option Card Configuration at the device	Controls a user's ability to access the "Option Card Menu" that displays menu nodes associated with installed DLEs	Any authorization option may be configured
Option Card Configuration Remotely	Controls a user's ability to access the "Option Card Menu" via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)

Item	Description	Comment
Paper Menu at the device (and submenus)	Controls access to the Paper Menu via the Administration Menus	Any authorization option may be configured
Paper Menu Remotely	Controls access to the Paper Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
PJL Device Setting Changes	When "Disabled", prohibits any changes to system settings via PJL operators	Must be disabled in the evaluated configuration
Release Held Faxes	Controls access to the Held Faxes button and the Release Held Faxes button on the Home screen	Access must be restricted to authorized administrators in the evaluated configuration
Remote Management	Controls whether or not management functions may be invoked from remote IT systems	Must be disabled in the evaluated configuration
Reports Menu at the device (and submenus)	Controls access to the Reports Menu via the Administration Menus. This includes information about user jobs, which can't be disclosed to non-administrators.	Access must be restricted to authorized administrators in the evaluated configuration
Reports Menu Remotely	Controls access to the Reports Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Security Menus at the device (and submenus)	Controls access to the Security Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Security Menu Remotely	Controls access to the Security Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Service Engineer Menus at the device (and submenus)	Controls access to any SE menu accessible from the panel, including the Network SE menu	Access must be restricted to authorized administrators in the evaluated configuration Note that LDAP+GSSAPI and PKI authentication may not be used with this access control because the network interface is not operational when these menus are in use
Service Engineer Menus Remotely	Controls access to any SE menu accessible from the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Settings Menu at the device (and submenus)	Controls access to the Settings Menu via the Administration Menus	Access must be restricted to authorized administrators in the evaluated configuration
Settings Menu Remotely	Controls access to the Settings Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Solution 1	Controls access to the Held Jobs menu if the "PKI Held Jobs" LES application is installed	Access must be restricted to authorized users in the evaluated configuration

Item	Description	Comment
Solution [x] (where x is any number other than 1)	Controls the execution of eSF and LDD profiles that specify using one of these slots	Configuration is unused; the only add-on Java applications included in the evaluated configuration use Solution 1.
Supplies Menu at the device (and submenus)	Controls access to the Supplies Menu via the Administration Menus	Any authorization option may be configured
Supplies Menu Remotely	Controls access to the Supplies Menu via the web	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)
Use Profiles	Controls a user's ability to execute any profile	Any authorization option may be configured
Web Import/Export Settings	Protects the Import/Export link in the Settings section of the AIO's Web page and all links beneath the Import/Export link	Configuration is ignored and function is implicitly disabled when HTTP server is disabled (which is the evaluated configuration)

Authorization is restricted by associating a security template with an item. The security template assigned to each item may be the same or different as the security template(s) assigned to other items. Each security template points to an authentication building block as well as an authorization building block; the two building blocks may be the same or different.

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

When a function is restricted by a security template, the access control function first determines if the user has already authenticated against the building block contained in the security template. If the user authenticated previously (during the current session), the name of the building block used during that authentication process was cached and can be compared to the name of the building block for this security template. If they match, the authentication step is skipped. Otherwise, if an authentication for a different building block was successfully performed during the current session, the username and password cached from that interaction is re-used for this authentication process against the authentication building block for this security template. If no authentication has already been done for this session, the I&A function is performed before access control continues.

Further access control processing is dependent on the type of authorization building block contained in the security template.

7.1.3.1 Internal Account Building Blocks

The set of groups configured for the Internal Account (and bound to the session during the I&A function) is compared to the set of groups included in the security template. If there are any common groups in those sets, the access control check is satisfied and the user is granted access to the requested function.

7.1.3.2 LDAP+GSSAPI and PKI Auth Building Blocks

For each group specified in the authorization building block, the LDAP server is queried to determine if the user is a member of the group. If the user is a member of any of those groups, the access control check is satisfied and the user is granted access to the requested function.

7.1.3.3 Common Processing

The information applies in this section applies to all types of building blocks.

If the access control check fails for an operation being performed at the UI, a message is displayed then the UI display is returned to the previous screen.

An audit record is generated with the result of the access control check.

7.1.3.4 Function Access Control

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

Table 27 - TOE Function Access Control SFP Rules

Object	Access Control Rules	Configuration Parameter Rules
F.PRT	Network print jobs can always be submitted if the submitted print job includes a userid in a SET USERNAME PJL statement. The job is held until released by a user who is a member of an authorized group for the Solution 1 or Held Jobs Access access control and has the same userid as was specified in the SET USERNAME PJL statement. Allowed for incoming faxes if the Fax Function access control is not "disabled".	Allowed Allowed if the "Enable Fax Receive" or "Enable Analog Receive" parameter is "On".
F.SCN	Allowed for fax if the user is a member of an authorized group of the security template configured for the Fax Function access control Allowed for copying if the user is a member of an authorized group of the security template configured for the Copy Function access control Allowed for emailing if the user is a member of an authorized group of the security template configured for the Fax Function access control	Allowed if the "Enable Fax Scans" parameter is On and the "Fax Mode" parameter is "Analog Fax" Allowed Allowed if the "Enable Fax Scans" parameter is On and the "Fax Mode" parameter is "Fax Server"
F.CPY	Allowed if the user is a member of an authorized group of the security template configured for the Copy Function access control In addition, color copying is allowed if the	Allowed Allowed

Object	Access Control Rules	Configuration Parameter Rules
	Copy Color Printing access control is "No security" or if the user is a member of an authorized group	
F.FAX	Incoming faxes are not subject to access control. All incoming faxes are held until released by a user who is a member of an authorized group of the security template configured for the Release Held Faxes access control Allowed for outgoing fax if the Fax Function access control is "No security" or if the user is a member of an authorized group	Allowed if the "Enable Fax Receive" or "Enable Analog Receive" parameter is "On". Allowed
F.SMI	Allowed provided the individual function access control allowed the function	Allowed

7.1.3.4.1 Printing

Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded. Submitted jobs are always held on the TOE until released or deleted by a user authorized for the appropriate access control and whose userid matches the username specified when the job was submitted. Users are able to display the queue of their pending print jobs. When a job is released, the user has the option to change the number of copies to be printed. If a held job is not released within the configured expiration time, the job is automatically deleted.

7.1.3.4.2 Scanning (to Fax or Email)

Scanning may be performed as part of a fax or email function. Only authorized users may perform scans.

The destination of the fax scan is determined by the setting of the "Fax Mode" configuration parameter. If it is configured for "Analog Fax" then the scanned data is transmitted out the phone line as a fax. If it is configured for "Fax Server" then the scanned data is forwarded to the configured email server via SMTP.

Scanning for fax is allowed if the Enable Fax Scans configuration parameter is "On" and the user is authorized for the Fax Function access control.

Scanning for email is allowed if the user is authorized for the E-mail Function access control.

7.1.3.4.3 Copying

Copying is allowed if the user is authorized for the Copy Function access control. A user may view or delete their own copy jobs queued for printing.

7.1.3.4.4 Incoming Fax

Incoming faxes are allowed if the "Enable Fax Receive" (for analog fax mode) or "Enable Fax Receive" (for fax server mode) configuration parameter is "On".

Incoming faxes are always held in the queue (until released) in the evaluated configuration. Only users authorized for the Release Held Faxes access control may release or delete the faxes.

7.1.3.4.5 Shared-medium Interface

The TOE supports scanning to an external SMTP server via the network interface. When fax functionality is enabled and the "Fax Mode" is configured for "Fax Server" outgoing faxes are converted to a file and attached to outgoing SMTP messages. Administrators require access to the Security Menu to configure the Fax Function access control and the Settings Menu to configure the fax server parameters.

7.1.3.5 Postscript Access Control

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

7.1.4 Management

The TOE provides the ability for authorized administrators to manage TSF data. Authorization is granular, enabling different administrators to be granted access to different TSF data. When an administrator modifies TSF data, an audit record is generated.

The following sections describe the management capabilities provided and are organized by the administrator menu structure available via the touch panel.

7.1.4.1 Reports Menu

The Reports menu provides the ability to print (view) the settings from other menu items as well as fax job logs (F.FUNC). This information must be restricted to authorized administrators.

7.1.4.2 Network/Ports Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 28 - Network/Ports Menu TSF Data

Item	Description	Comments
Network Port	Defines the parameters required for the TOE to communicate via the standard network port	Required if the TOE supports network-attached users or if LDAP+GSSAPI or PKI authentication is used
Enable FTP/TFTP	Enables FTP/TFTP server on the TOE	Must be disabled in the evaluated configuration
Enable HTTP Server	Enables HTTP(S) server on the TOE	Must be disabled in the evaluated configuration
USB Buffer	Disables all activity via the USB port	Must be disabled in the evaluated configuration
SMTP Setup Settings	Define the SMTP server to be used to send email from the TOE	Required if the TOE supports scan to email or fax to email
SMTP Setup Settings - User-Initiated E-mail	None (*) Use Device SMTP Credentials Use Session User ID & Password Use Session E-mail & Password Prompt User	Any option other than "None" may be configured in the evaluated configuration

7.1.4.3 Security Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 29 - Security Menu TSF Data

Item	Description	Comments
Edit Backup Password - Use Backup Password	Enables access to the Security Menu via the Backup Password	Only appears if backup password exists. Enabling the backup password is optional.
Edit Backup Password - Password	Specifies the Backup Password	The TOE requires passwords to be a minimum of 8 characters, with no composition rules. Operational guidance directs administrators to use the following composition rules when specifying passwords: at least one upper case letter, one lower case letter, and one non-alphabetic character; no dictionary words or permutations of the username
Edit Building Blocks - Internal Accounts - General Settings - Required User Credentials	User ID and password (*) User ID	"User ID and password" is required in the evaluated configuration
Edit Building Blocks - Internal Accounts - General Settings - Groups	Defines the groups that may be associated with users, Internal Account building blocks, and security templates (using Internal Accounts)	Required if Internal Account building blocks are used
Edit Building Blocks - Internal Accounts – Manage Internal Accounts	Defines the account name, username, password, email address, and associated groups for each internal account	The TOE requires passwords to be a minimum of 8 characters, with no composition rules. Operational guidance directs administrators to use the following composition rules when specifying passwords: at least one upper case letter, one lower case letter, and one non-alphabetic character; no dictionary words or permutations of the username
Edit Building Blocks - Simple Kerberos Setup - KDC Address, KDC Port, and Realm	Defines how to communicate with the KDC	Required if LDAP+GSSAPI or PKI authentication (without PKI-specific Kerberos parameters in the PKI Auth building block) is being used since they use a Kerberos Building Block in order to define the parameters for communication with the KDC
Edit Building Blocks - LDAP+GSSAPI	Defines how to communicate with the LDAP server and (optionally) restrict the groups and users that will match the query	Required if LDAP+GSSAPI is being used to define the LDAP server to be used
Edit Building Blocks - LDAP+GSSAPI – Certificate	default (*) Certificate	The evaluated configuration requires the default certificate if SSL/TLS is selected in the building block.
Edit Building Blocks - LDAP+GSSAPI – Device Credentials	Distinguished username and password to be used when performing LDAP queries	Required in the evaluated configuration

Item	Description	Comments
Access Controls	Specifies whether access is no security, disabled, or restricted for each item (see the Access Control security function for the list of items)	Refer to the Access Control security function for requirements on access controls
Login Restrictions	The "Login failures" value determines how many failed authentications (local OR remote) are allowed within the "Failure time frame" value before the offending User Name is prevented from accessing any function protected with the same building block (e.g. LDAP, Kerberos, etc.) for the duration of the "Lockout time" value. The value of "Panel Login Timeout" determines how long the operator panel can remain idle on the Home screen before the user is logged off automatically.	Any configuration options may be configured. The lockout function is always enabled and any settings within the allowed range will result in a configuration with adequate security against brute force password attacks.
Security Reset Jumper	No Effect No Security (*) Reset to Defaults	"No Security" preserves all of the building blocks and templates that a user has defined, but resets each access control to its factory default security level. "Reset to Defaults" deletes all building blocks and templates that a user has defined and resets each access control to its factory default security level.
LDAP Certificate Verification	Demand (*) Try Allow Never	"Demand!" must be configured in the evaluated configuration
Wiping Mode	Controls the mode used for disk wiping Off (*) Automatic Manual	"Automatic" must be specified in the evaluated configuration
Automatic Method	Specifies the method used for automatic disk wiping Single pass (*) Multiple pass	"Multiple pass" must be specified in the evaluated configuration
Enable Audit	Determines if the device records events in the secure audit log and (if enabled) in the remote syslog Yes No (*)	Any configuration options may be configured.
Enable Remote Syslog	Determines if the device transmits logged events to a remote server Yes No (*)	"Yes" must be specified in the evaluated configuration
Remote Syslog parameters	Defines the communication to the remote syslog system	Must be configured in the evaluated configuration.

Item	Description	Comments
Date and Time parameters	Controls whether the time is tracked internally or from a remote NTP server	Must be configured for either local or remote operation so that the TOE can provide timestamps in audit records
Held Print Job Expiration Timer	Specifies the maximum amount of time a print job is held while waiting for a user to release it for printing Off 1 hour 4 hours 24 hours 1 week	Any configuration option may be configured.

When an Internal Account is defined, initially no groups are associated with it. The TOE limits the specification of group memberships to defined groups. If a group is associated with any Internal Accounts, the group may not be deleted.

7.1.4.4 Settings Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 30 - General Settings Menu TSF Data

Item	Description	Comments
FTP	Display (*) Do not display	Must be set to "Do not display" in the evaluated configuration
FTP shortcuts	Display (*) Do not display	Must be set to "Do not display" in the evaluated configuration
USB Drive	Display (*) Do not display	Must be set to "Do not display" in the evaluated configuration

7.1.4.4.1 Fax Settings Menu

Analog fax mode uses a phone line connected directly to the MFP to send and/or receive faxes. In fax server mode, scanned documents are forwarded to a fax server via SMTP rather than being transmitted out the fax interface; a fax line may still be connected to process incoming faxes. The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 31 - Fax Settings Menu TSF Data

Item	Description	Comments
Fax Mode	Analog Fax Server	Any configuration option may be specified
Cancel Faxes	Allow (*) Don't Allow	Any configuration option may be specified, according to local policy concerning faxes.
Enable Fax Scans	On (*) Off When "On", user can create faxes with the device's scanner.	Any configuration option may be specified, according to local policy concerning scan to fax usage.

Item	Description	Comments
Driver to fax	Yes (*) No When "No", driver fax jobs are treated as PS jobs. This is the only way to disable "Driver to fax"	"No" must be specified in the evaluated configuration
Enable Fax Receive	Specifies whether incoming faxes may be received On (*) Off	Any configuration option may be specified, according to local policy concerning received faxes.
Fax Forwarding	Print (*; fax forwarding off, print all received faxes) Print and Forward Forward	"Print" must be configured in the evaluated configuration.
Holding Faxes	Defines conditions for holding incoming faxes.	In the evaluated configuration, the conditions must be configured so that all incoming faxes are held.
Enable Analog Receive	Off (*) On This parameter controls whether incoming faxes are supported when operating in fax server mode	Any configuration option may be specified, according to local policy concerning incoming faxes.

7.1.4.4.2 Email Settings Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 32 - Email Settings Menu TSF Data

Item	Description	Comments
E-mail images sent as	Attachment (*) Web link	"Attachment" must be specified in the evaluated configuration

7.1.4.4.3 Print Settings/Setup Settings Menu

The following table describes TSF data available for management under this menu. In the description field, "(*)" indicates the default setting for an item.

Table 33 - Print Settings/Setup Settings Menu TSF Data

Item	Description	Comments
Job Waiting	On Off (*)	Any configuration option may be specified

7.1.4.5 Security Reset Jumper

The security reset jumper provides an alternate mechanism to manage some TSF data. The TOE contains a hardware jumper that can be used to:

- erase all security templates, building blocks, and access controls that a user has defined (i.e. the factory default configuration); OR
- force the value of each function access control to "No Security" (all security templates and building blocks are preserved but not applied to any function).

Administrators can secure the hardware containing the jumper with a Kensington lock. Or, to completely negate the effects of a jumper reset, an authorized administrator can configure the TOE to take no action based upon the jumper, effectively disabling this mechanism. Authorized administrators use the same configuration parameter to determine which of the two actions listed above is performed (if the mechanism is not disabled).

To perform a jumper reset operation, an administrator:

1. powers the device off;
2. removes the Kensington lock from the card cage;
3. removes the small plastic piece that covers a pair of the jumper's pins;
4. replaces the plastic piece so that it covers the pins adjacent to its original position;
5. replaces and secures the Kensington lock on the card cage;
6. powers the device on.

The movement of the plastic piece from position A to position B on the jumper triggers the reset, not the specific positions. When the TOE is powered on, it labels the current position of the plastic piece as the "home" position. If, at the next power on or reset, the TOE detects that the plastic piece has moved from its previous "home" position to the "other" position, then it performs the jumper reset operation. After performing the operation, the TOE also relabels the "other" position as the "home" position.

7.1.5 Operator Panel Lockout

The Operator Panel Lockout function enables the touch panel to be "locked" to prevent anyone from using it until it is "unlocked" by an authorized user. This function is enabled when a security template is associated with the Operator Panel Lock access control described above. When enabled, an icon is displayed on the Home page to lock the panel.

When that lock icon is touched, the user must authenticate (if not already authenticated). If I&A is successful, the device is locked and the current session is terminated immediately. When locked, the only icon appearing on the touch panel is to unlock the MFP.

When the unlock icon is touched, the user must authenticate. If I&A is successful, the touch panel is unlocked and the Home page is displayed. The current session is immediately terminated, requiring a user to authenticate again before any controlled function may be accessed.

7.1.6 Fax Separation

The Fax Separation 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 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 (in the evaluated configuration) is a document that was scanned for faxing.

In the evaluated configuration, the USB ports capable of being used for document input are disabled and the ability to submit jobs via the network interface to be sent out the fax interface is disabled. Therefore, the only source for outgoing fax transmissions is the scanner. Control of the fax functionality is incorporated directly into the TOE's firmware. The modem chip is in a mode that is more restrictive than Class 1 mode (the fax modem will not answer a data call), 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 used over the analog fax line.

The fax 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. The modem and the network adapter are incapable of communicating 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.

7.1.7 Hard Disk Encryption

All user data saved on the Hard Disk is encrypted using 256-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. The key is generated using the internal random number generator 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:

1. Disabling the hard disk encryption feature - the encryption key is zeroized.
2. Enabling the hard disk encryption feature when it is already enabled - a new encryption key is generated; the previous key is zeroized.

7.1.8 Disk Wiping

In the evaluated configuration, the TOE is configured to perform automatic disk wiping with a multi-pass method. Files containing user data are stored on the internal hard drive until they are no longer needed. At that time, they are logically deleted and marked as needing to be wiped. Until the wiping occurs, the disk blocks containing the files are not available for use by any user. Every 5 seconds, the TOE checks to see if any "deleted" files are present and begins the disk wiping process.

The TOE overwrites each block associated with each deleted file (including bad and remapped sectors) three times: first with "0x0F" (i.e. 0000 1111), then with "0xF0" (i.e. 1111 0000), and

finally with a block of random data (supplied by the internal random number generator). Each time that the device wipes a different file, it selects a different block of random data. This method is compliant with NIST SP800-88 and the DSS "Clearing and Sanitization Matrix" (C&SM).

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

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

The TOE also overwrites RAM with a fixed pattern upon deallocation of any buffer used to hold user data.

7.1.9 Secure Communications

IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are TDES, AES and DES. Both SHA-1 and MD5 are supported for HMACs.

ISAKMP and IKE are used to establish the Security Association (SA) and session keys for the IPSec exchanges. Diffie-Hellman is used for key agreement, using Oakley Groups 1, 2 or 14. During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature for it is validated.

If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded.

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

The TOE zeroizes the session keys when the sessions are terminated.

7.1.10 Self Test

During initial start-up, the TOE performs self tests on the hardware. The integrity of the security templates and building blocks is verified by ensuring that all the security templates specified in access controls exist and that all building blocks referenced by security templates exist.

If any problems are detected with the hardware, an appropriate error message is posted on the touch screen and operation is suspended. If a problem is detected with the integrity of the security templates or building blocks, the data is reset to the factory default, an audit log record is generated, an appropriate error message is posted on the touch screen, and further operation is suspended. In this case, a system restart will result in the system being operational with the factory default settings for the data.

8. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 2.

8.1 TOE Type Consistency

Both the PP and the TOE describe Hard Copy Devices.

8.2 Security Problem Definition Consistency

This ST claims demonstrable conformance to the referenced PP.

All of the assumptions, threats, and organizational security policies of the PP are included in the ST. One additional assumption (A.IPSEC) is included in the ST, resulting in the ST being more restrictive than the PP.

8.3 Security Objectives Consistency

This ST claims demonstrable conformance to the referenced PP.

All of the security objectives for the TOE and the operational environment (IT and non-IT) of the PP are included in the ST. The following additional security objectives are included in the ST:

1. O.I&A
2. O.MANAGE
3. O.TIME_STAMP
4. OE.I&A
5. OE.IPSEC
6. OE.TIME_STAMP

Therefore, the ST is more restrictive than the PP.

8.4 Security Functional Requirements Consistency

This ST claims demonstrable conformance to the referenced PP.

All of the SFRs from the claimed SFR packages are included in the ST with any fully or partially completed operations from the PP. Any remaining operations have been completed. The following notes apply to conformance of the SFRs in the ST.

1. The auditable events listed in the table with FAU_GEN.1 have been enumerated to match the specific events generated by the TOE. All of the events required by the PP are represented along with additional events.
2. SFRs from the FCS class have been added to the ST to address cryptographic functionality for IPSec and disk encryption, which are additions to the security functionality required by the PP.
3. FDP_ACC.1(a) and FDP_ACF.1(a) have been integrated with the individual instances of FDP_ACC.1 and FDP_ACF.1 from the applicable SFR packages of the PP into a single instance of FDP_ACC.1 and FDP_ACF.1 (still named Common Access Control SFP) that addresses all of the access control policies.

4. FDP_ACC.1(c) and FDP_ACF.1(c) have been added to the ST to address an access control function (touch panel locking) that is an addition to the security functionality required by the PP.
5. FIA_AFL.1 has been added to the ST to address to address authentication failure handling, which is an addition to the security functionality required by the PP.
6. FIA_UAU.7 has been added to the ST to address to address protected authentication feedback, which is an addition to the security functionality required by the PP.
7. FMT_MSA.1(a) and FMT_MSA.1(b) from the PP were combined into a single instance of FMT_MSA.1 since all the completed operations were identical.
8. FMT_MSA.3(a) and FMT_MSA.3(b) from the PP were combined into a single instance of FMT_MSA.3 since all the completed operations were identical.
9. FMT_MTD.1(a) and FMT_MTD.1(b) from the PP were combined into a single instance of FMT_MTD.1. Users (U.NORMAL) do not have any access to TSF data, and it was necessary to provide permission-level granularity of the administrator role for various TSF data access. Given these conditions, it was simpler to combine the instances of FMT_MTD.1 in the ST.
10. For FMT_SMR.1, the TOE provides greater granularity of roles based on individual permissions that is required by the PP. The permission-based description has been provided in the ST, and an application note with the SMR defines the relationship between those permissions and the roles defined by the PP.
11. The instance of the FAU_GEN.1 in the SMI package has been integrated with the instance of FAU_GEN.1 in the common requirements.

8.5 Security Assurance Requirements Consistency

The ST assurance claims are identical to the assurance claims of the PP.

9. 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.

9.1 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, policy and assumption is addressed by a security objective.

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

Table 34 - Threats, Policies and Assumptions to Security Objectives Mapping

	O.AUDIT.LOGGED	O.CONF.NO_ALT	O.CONF.NO_DIS	O.DOC.NO_ALT	O.DOC.NO_DIS	O.FUNC.NO_ALT	O.INTERFACE.MANAGED	O.I&A	O.MANAGE	O.PROT.NO_ALT	O.SOFTWARE.VERIFIED	O.TIME_STAMP	O.USER.AUTHORIZED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.AUDIT.REVIEWED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT_STORAGE.PROTECTED	OE.I&A	OE.INTERFACE.MANAGED	OE.IPSEC	OE.PHYSICAL.MANAGED	OE.TIME_STAMP	OE.USER.AUTHORIZED	OE.USER.TRAINED
A.ACCESS.MANAGED																						X			
A.ADMIN.TRAINING														X											
A.ADMIN.TRUST															X										
A.IPSEC																					X				
A.USER.TRAINING																									X
T.CONF.ALT		X						X					X						X					X	
T.CONF.DIS			X					X					X						X					X	
T.DOC.ALT				X				X					X						X					X	
T.DOC.DIS					X			X					X						X					X	
T.FUNC.ALT						X		X					X						X					X	
T.PROT.ALT								X		X			X						X					X	
P.AUDIT.LOGGING	X											X				X	X	X					X		
P.INTERFACE.MANAGEMENT							X													X	X				
P.SOFTWARE.VERIFICATION											X														
P.USER.AUTHORIZATION								X	X				X						X					X	

9.1.1 Rationale Showing Threats to Security Objectives

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

Table 35 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.CONF.ALT	O.CONF.NO_ALT – The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of TSF Confidential Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.CONF.DIS	O.CONF.NO_DIS - The objective addresses the threat by requiring the TOE to protect against unauthorized disclosure of TSF Confidential Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.DOC.ALT	O.DOC.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of User Document Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.DOC.DIS	O.DOC.NO_DIS - The objective addresses the threat by requiring the TOE to protect against unauthorized disclosure of User Document Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.FUNC.ALT	O.FUNC.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of User Function Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.
T.PROT.ALT	O.PROT.NO_ALT - The objective addresses the threat by requiring the TOE to protect against unauthorized alteration of TSF Protected Data. O.I&A and OE.I&A – The objectives help address the threat by requiring I&A mechanisms so that appropriate authorizations may be associated with users. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the threat by requiring authorizations to be specified for users.

9.1.2 Rationale Showing Policies to Security Objectives

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

Table 36 - Policies to Security Objectives Rationale

P.TYPE	Security Objectives Rationale
P.AUDIT.LOGGING	O.AUDIT.LOGGED – The objective addresses the first part of the policy by requiring the TOE to generate audit records for TOE usage and security-relevant events, and to protect these records while they are inside the TSC. O.TIME_STAMP – The objective supports the policy by requiring the TOE to provide time stamps for the audit records when time is being tracked internally. OE.AUDIT.REVIEWED – The objective addresses the audit review portion of the policy by requiring timely review of the generated audit records. OE.AUDIT_ACCESS.AUTHORIZED – The objective supports the policy by requiring the operational environment to make the audit records available to authorized personnel only. OE.AUDIT_STORAGE.PROTECTED - The objective supports the policy by requiring the operational environment to protect the stored audit records from unauthorized access. OE.TIME_STAMP - The objective supports the policy by requiring the TOE to provide time stamps for the audit records when time is being supplied externally.
P.INTERFACE.MANAGEMENT	O.INTERFACE.MANAGED – The objective addresses the policy by requiring the TOE to enforce access to and usage of the TOE interfaces within the TSC. OE.INTERFACE.MANAGED – The objective addresses the policy by requiring the operational environment to control access to the TOE interfaces within the operational environment.
P.SOFTWARE.VERIFICATION	O.SOFTWARE.VERIFIED – The objective restates the policy.
P.USER.AUTHORIZATION	O.I&A and OE.I&A – The objectives help address the policy by requiring I&A mechanisms so that user authorizations may be restricted for users. O.MANAGE – The objective addresses the policy by requiring the TOE to provide management functions to administrators for configuration of user authorizations. O.USER.AUTHORIZED and OE.USER.AUTHORIZED – The objectives help address the policy by requiring authorizations to be specified for users.

9.1.3 Rationale Showing Assumptions to Environment Security Objectives

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

Table 37 - Assumptions to Security Objectives Rationale

A.TYPE	Security Objectives Rationale
A.ACCESS.MANAGED	OE.PHYSICAL.MANAGED – The objective addresses the assumption by requiring the TOE to be located in an area that restricts physical access.
A.ADMIN.TRAINING	OE.ADMIN.TRAINED – The objective restates the assumption.
A.ADMIN.TRUST	OE.ADMIN.TRUSTED – The objective addresses the assumption by requiring trust to be established in the administrators.
A.IPSEC	OE.IPSEC – All network systems with which the TOE communicates are required to support IPSec with ESP.
A.USER.TRAINING	OE.USER.TRAINED – The objective restates the assumption.

9.2 Security Requirements Rationale

9.2.1 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 38 - SFRs to Security Objectives Mapping

	O.AUDIT.LOGGED	O.CONF.NO_ALT	O.CONF.NO_DIS	O.DOC.NO_ALT	O.DOC.NO_DIS	O.FUNC.NO_ALT	O.INTERFACE.MANAGED	O.I&A	O.MANAGE	O.PROT.NO_ALT	O.SOFTWARE.VERIFIED	O.TIME_STAMP	O.USER.AUTHORIZED
FAU_GEN.1	X											X	
FAU_GEN.2	X												
FCS_CKM.1(A)					X								
FCS_CKM.1(B)					X								
FCS_CKM.4					X								
FCS_COP.1					X								
FDP_ACC.1(A)				X	X	X	X			X			X
FDP_ACC.1(B)				X	X	X	X			X			X
FDP_ACC.1(C)							X						X
FDP_ACF.1(A)				X	X	X	X			X			X
FDP_ACF.1(B)				X	X	X	X			X			X
FDP_ACF.1(C)							X						X
FDP_RIP.1					X								
FIA_AFL.1								X					
FIA_ATD.1								X					
FIA_UAU.1								X					X
FIA_UAU.7								X					
FIA_UID.1								X					X
FIA_USB.1								X					X
FMT_MOF.1		X	X						X				X
FMT_MSA.1		X	X						X				X
FMT_MSA.3									X				
FMT_MTD.1		X	X						X				X
FMT_SMF.1									X				
FMT_SMR.1									X				
FPT_FDI_EXP.1							X		X				
FPT_STM.1												X	
FPT_TST.1											X		
FTA_SSL.3									X				
FTP_ITC.1					X								

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

Table 39 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT.LOGGED	FAU_GEN.1 addresses the objective by requiring the TOE to generate audit records for TOE usage and security relevant events. FAU_GEN.2 helps address the objective by requiring the audit records to include information associating a user with each event (if applicable).
O.CONF.NO_ALT	FMT_MOF.1 specifies the rules for managing the behaviour of security-relevant functions, which is done by altering TSF Confidential Data and should only be accessed by authorized administrators. FMT_MSA.1 specifies the rules for managing user security attributes used in user data access control decisions, which is done by altering TSF Confidential Data and should only be accessed by authorized administrators. FMT_MTD.1 specifies the rules for altering TSF Confidential Data.
O.CONF.NO_DIS	FMT_MOF.1 specifies the rules for managing the behaviour of security-relevant functions, which includes displaying TSF Confidential Data and should only be accessed by authorized administrators. FMT_MSA.1 specifies the rules for managing user security attributes used in user data access control decisions, which includes displaying TSF Confidential Data and should only be accessed by authorized administrators. FMT_MTD.1 specifies the rules for displaying TSF Confidential Data.
O.DOC.NO_ALT	FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding User Document Data that must be protected for unauthorized alteration. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted.
O.DOC.NO_DIS	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 support the objective by requiring the TOE to provide key management and cryptographic functions to protect the document data during network transmission and while stored on the TOE's hard disk. FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding User Document Data that must be protected for unauthorized disclosure. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted. FDP_RIP.1 supports the objective by requiring the TOE to make unavailable any user document data when a user job completes. FTP_ITC.1 addresses the objective by requiring the TOE to provide trusted channels for the exchange of document data across the network.
O.FUNC.NO_ALT	FDP_ACC.1(A) specifies the subjects, objects and operations that are controlled regarding functions. FDP_ACF.1(A) specifies the security attributes and rules used to determine whether access is permitted.
O.INTERFACE.MANAGED	FDP_ACC.1(A), FDP_ACC.1(B) and FDP_ACC.1(C) specify the subjects, objects and operations that are controlled regarding all TOE interfaces. FDP_ACF.1(A), FDP_ACF.1(B) and FDP_ACF.1(C) specify the security attributes and rules used to determine whether access is permitted. FPT_FDI_EXP.1 specifies that the TOE restrict the flow of information between the network and fax interfaces.
O.I&A	FIA_AFL.1 supports the objective by requiring the TOE to lock accounts that experience an excessive number of failed authentication attempts, thereby providing protection from brute force password attacks. FIA_ATD.1 specifies the attributes associated with users, including information

Security Objective	SFR and Rationale
	about failed authentication attempts. FIA_UAU.1 requires the TOE to provide I&A using Internal Accounts and the Backup Password. FIA_UAU.7 protects the confidentiality of passwords by specifying that only asterisks are echoed during password entry. FIA_UID.1 requires the TOE to provide I&A using Internal Accounts and the Backup Password. FIA_USB.1 specifies the attributes bound to a session upon successful completion of the I&A process.
O.MANAGE	FPT_FDI_EXP.1 requires the TOE to provide management of direct forwarding from the original document handler input to the network interface. FMT_MOF.1 specifies the rules for administrator access to the listed functions. FMT_MSA.1 specifies the rules for management of the security attributes used in the access control decisions for user data. FMT_MSA.3 requires the TOE to impose restrictive default values for security attributes in all cases. FMT_MTD.1specifies the rules for management of TSF data. FMT_SMF.1 specifies the management functions that the TOE provides and controls access to. FMT_SMR.1 specifies the two roles supported by the TOE.
O.PROT.NO_ALT	FDP_ACC.1(A) and FDP_ACC.1(B) specify the subjects, objects and operations that are controlled regarding TSF Protected Data that must be protected for unauthorized alteration. FDP_ACF.1(A) and FDP_ACF.1(B) specify the security attributes and rules used to determine whether access is permitted.
O.SOFTWARE.VERIFIED	FPT_TST.1 addresses the objective by requiring the TOE to validate the TSF data for security templates and building blocks.
O.TIME_STAMP	FPT_STM.1 requires the TOE to provide a reliable time source when time is configured to be supplied internally.
O.USER.AUTHORIZED	FIA_UID.1 and FIA_UAU.1 requires the TOE to successfully complete the I&A process before allowing users to perform anything other than the specified functions. FIA_USB.1 specifies the attributes bound to a sessions (and used in access control decisions) upon successful I&A. The security policies defined in FDP_ACC.1(A), FDP_ACC.1(B), FDP_ACC.1(C), FDP_ACF.1(A), FDP_ACF.1(B), FDP_ACF.1(C), FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 are required to be enforced by the TOE based on the security attributes bound to the subject (acting on behalf of the authenticated user).

9.2.2 Security Assurance Requirements Rationale

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 EAL3 augmented with ALC_FLR.2 from part 3 of the Common Criteria.

9.3 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 40 - SFRs to TOE Security Functions Mapping

	Audit Generation	I&A	Access Control	Management	Touch Panel Lockout	Fax Separation	Hard Disk Encryption	Disk Wiping	Secure Communication	Self Test
FAU_GEN.1	X									
FAU_GEN.2	X									
FCS_CKM.1(A)							X			
FCS_CKM.1(B)									X	
FCS_CKM.4							X		X	
FCS_COP.1							X	X	X	
FDP_ACC.1(A)			X							
FDP_ACC.1(B)			X							
FDP_ACC.1(C)					X					
FDP_ACF.1(A)			X							
FDP_ACF.1(B)			X							
FDP_ACF.1(C)					X					
FDP_RIP.1								X		
FIA_AFL.1		X								
FIA_ATD.1		X								
FIA_UAU.1		X								
FIA_UAU.7		X								
FIA_UID.1		X								
FIA_USB.1		X								
FMT_MOF.1			X	X						
FMT_MSA.1			X	X						
FMT_MSA.3				X						
FMT_MTD.1			X	X						
FMT_SMF.1				X						
FMT_SMR.1				X						
FPT_FDI_EXP.1			X	X		X				
FPT_STM.1	X									
FPT_TST.1										X
FTA_SSL.3		X								
FTP_ITC.1									X	

Table 41 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	Audit Generation addresses the SFR by specifying the audit event records that are generated and the content of the records.
FAU_GEN.2	Audit Generation addresses the SFR by specifying that the associated Username (if applicable) is included in audit event records.
FCS_CKM.1(A)	Hard Disk Encryption generates a key used to encrypt the files on the hard disk when this function is enabled.
FCS_CKM.1(B)	Secure Communications requires generation of a certificate with an RSA public-private key pair.
FCS_CKM.4	Hard Disk Encryption requires the key used to encrypt the files on the hard disk to be zeroized when the function is disabled. Secure Communication requires zeroization of the session keys obtained by DH key agreement to be zeroized when the sessions terminate.
FCS_COP.1	Hard Disk Encryption uses the random number generator and AES to generate the key used to encrypt the files on the hard disk, and uses AES to perform the encryption and decryption. Disk Wiping uses the random number generator to obtain random data used during disk sanitization. Secure Communication requires the TOE to support TDES, AES and DES for encryption, AES and SHA-1 for HMAC, RSA signatures, Diffie Hellman for key agreement, and a pseudo-random number generator.
FDP_ACC.1(A)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACC.1(B)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACC.1(C)	Touch Panel Lockout specifies the access controls placed on the users for locking, unlocking and using the Touch Panel.
FDP_ACF.1(A)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACF.1(B)	Access Control specifies the access controls placed on the user operations (objects) performed by users to access user data in the TSC.
FDP_ACF.1(C)	Touch Panel Lockout specifies the access controls placed on the users for locking, unlocking and using the Touch Panel.
FDP_RIP.1	Disk Wiping requires the TOE to erase disk files and RAM buffers upon their release that contain user data from incoming print, copy, scan and fax jobs.
FIA_AFL.1	Identification and Authentication requires the TOE to track failed login attempts for all authentication mechanisms. The limit on failed attempts that triggers an account lock is specified via the Login Restrictions TSF data.
FIA_ATD.1	Identification and Authentication requires the TOE to maintain the Username, Password, and Associated Groups security attributes for Internal Accounts and the Backup Password; and the failed authentication security attributes for all users.
FIA_UAU.1	Identification and Authentication requires the TOE to prevent access to restricted functions before the I&A process is successfully completed. Printing is never a restricted function; other functions may be restricted through access controls or enabling/disabling specific functions such as incoming faxes. The TOE is solely responsible for I&A for Internal Accounts and the Backup Password.
FIA_UAU.7	Identification and Authentication requires the TOE to echo asterisks when a password is being entered for the I&A process for all mechanisms.

SFR	SF and Rationale
FIA_UID.1	Identification and Authentication requires the TOE to prevent access to restricted functions before the I&A process is successfully completed. Printing is never a restricted function; other functions may be restricted through access controls or enabling/disabling specific functions such as incoming faxes. The TOE is solely responsible for I&A for Internal Accounts and the Backup Password.
FIA_USB.1	Identification and Authentication requires the TOE to bind the Username and Password supplied during I&A with the subject upon successful I&A. The TOE also binds the list of associated groups (for Internal Accounts) and the building block name used for I&A.
FMT_MOF.1	Management requires the TOE to provide the management capabilities specified in the table to the administrators that satisfy the access controls associated with the menus that control those functions. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_MSA.1	Management requires the TOE to provide the management capabilities for Usernames and Group memberships to the administrators that satisfy the access controls associated with the menus that control access to the data items. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_MSA.3	Management requires the TOE to initially associate no group memberships with Internal Accounts.
FMT_MTD.1	Management requires the TOE to provide the management capabilities specified in the table to the administrators that satisfy the access controls associated with the menus that control access to the data items. Access Control specifies that access be restricted and states the required configuration in the evaluated configuration.
FMT_SMF.1	Management requires the TOE to provide capabilities to manage the specified functions.
FMT_SMR.1	Management requires the TOE to maintain the two specified roles. Administrators are any users authorized access to management functionality, while normal users are all the other defined users.
FPT_FDI_EXP.1	Access Control requires the TOE to prevent data from being forwarded from the original document handler interfaces to the network interface in the evaluated configuration un;ess authorized by an administrator. Management provides an administrator with the ability to configure the TOE for operation in this manner. Fax Separation requires the TOE to prevent any forwarding of data between the fax interface and the network port.
FPT_STM.1	Audit Generation requires the TOE to provide time stamps for audit records when the TOE is configured for internal time.
FPT_TST.1	Self Test requires the TOE to perform tests on the hardware and validate the security templates and building blocks on each power up and reset.
FTA_SSL.3	Identification and Authentication states that sessions are automatically terminated by the TOE when the Home menu is not accessed within the configured timeout period.
FTP_ITC.1	Secure Communication requires the TOE to use a trusted channel for network communication with all remote IT systems.

9.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 8.