Xerox WorkCentre™ 7525/7530/7535/7545/7556 Security Target Version 1.0

Prepared by:

Xerox Corporation
800 Phillips Road
Webster, New York 14580

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Document Version 1.0, Revision 1.4

Document Version: 1.0 (December 2011).

Table of Contents

List of Figures

List of Tables

1. SECURITY TARGET INTRODUCTION

This Chapter presents Security Target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4, 5 and 6, Security Objectives, Extended Components Definition, and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 7, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 11.

1.1.ST and TOE Identification

This section provides information needed to identify and control this ST and its associated TOE. This ST targets Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.3.

ST Title:	Xerox WorkCentre™ 7525/7530/7535/7545/7556 Security Target
ST Version:	1.0
Revision Number:	Revision 1.4
Publication Date:	December 7, 2011
Authors:	CSC Security Testing/Certification Laboratories, Xerox Corporation
TOE Identification:	Xerox WorkCentre™ 7525/7530/7535/7545/7556 (see Section 1.3.1 for software version numbers)

ST Evaluator:	CSC Security Testing/Certification Laboratories
Keywords:	Xerox, Multi Function Device, Image Overwrite, WorkCentre™, Color, Mono, 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, Network, Office, ISO/IEC 15408, Common Criteria, FIPS, Protection Profile, Security Target

1.2. TOE Overview

1.2.1. Usage and Major Security Features

The product is a multi-function device (MFD) that copies and prints in monochrome (black and white) and full color, with scan (including "scan-to-mailbox[1]"), and FAX options. A standard component of the TOE is the Image Overwrite Security package. This function forces any temporary image files created during a copy, print, scan or Fax job to be overwritten when those files are no longer needed. For reference, the architecture of the TOE is illustrated in Figure 1: Architectural Diagram of the TOE below:

[1] In Xerox terminology, the terms "mailbox" and "folder" are used interchangeably, both referring to logical place holders under which files are stored.

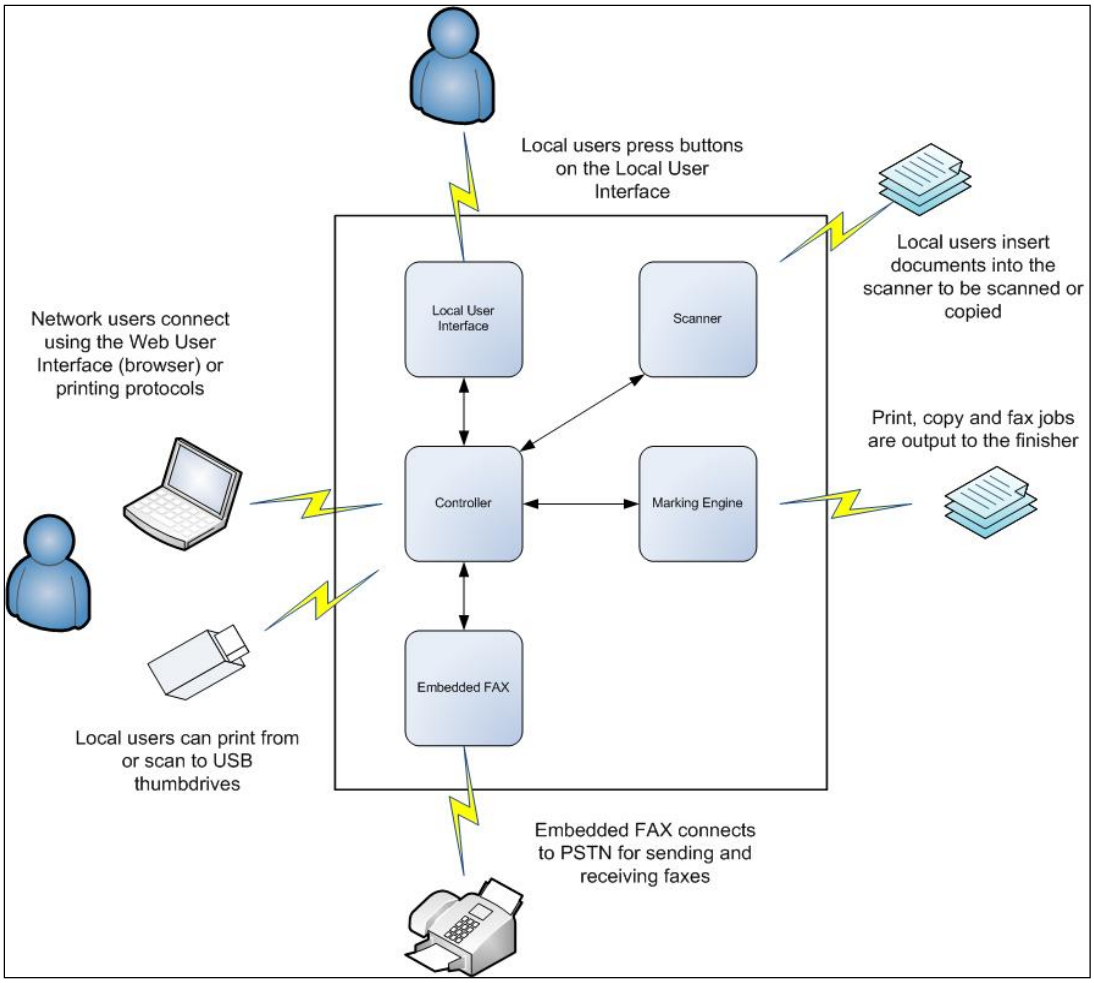


Figure 1: Architectural Diagram of the TOE

The optional Xerox Embedded Fax accessory, when purchased and installed, provides local analog fax capability over PSTN connections. Table 1 shows the configurations and printing speeds available in the various models of the TOE.

Table 1: Models and capabilities

(X – included in all configurations; O – product options ordered separately)

	Print	Copy	Scan	Fax	Print Speed (Color)	Print Speed (Mono)
WorkCentre™ 7525	x	x	x	o	Up to 25 ppm	Up to 25 ppm
WorkCentre ™ 7530	x	x	x	o	Up to 30 ppm	Up to 30 ppm
WorkCentre ™ 7535	x	x	x	o	Up to 35 ppm	Up to 35 ppm
WorkCentre ™ 7545	x	x	x	o	Up to 45 ppm	Up to 45 ppm
WorkCentre ™ 7556	x	x	x	o	Up to 50 ppm	Up to 55 ppm

The hardware included in the TOE is shown in the figure below.

Figure 2: Xerox WorkCentre™ 7525/7530/7535/7545/7556

The TOE stores temporary image data created during a copy, print, scan and Fax job on the single shared HDD. This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The encryption key is created on each power-up.

The TOE provides an Image Overwrite function to enhance the security of the MFD. The Image Overwrite function overwrites temporary document image data at the completion of each job; also upon deletion of each job or of a workflow scan/fax, file/mailbox in the following cases: at the instruction of the

owner; after a reboot; once the TOE is turned back on after a power failure/unorderly shutdown; or *on demand* of the TOE system administrator.

The optional Xerox Embedded Fax accessory provides analog FAX capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax jobs, if purchased by the consumer.

Xerox's Workflow Scanning Accessory is part of the TOE configuration. This accessory allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository, kept in a private (scan) mailbox or placed on to a personal USB storage device.

All models of the TOE support auditing. The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit records; the downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

All models of the TOE support network security. The system administrator can enable and configure the network security support. Filtering rules can be specified for IPv4 based on both address and port number. Additional security support is provided in the form of secure network communication protocols supported. SSL support is available for protecting communication over the Web User Interface (Web UI). SSL may be used for protecting document transfers to the remote file depository. IPSec support is available for protecting communication over IPv4 and IPv6. Kerberos or SSL support are available for protecting communication in support of remote authentication.

The TOE controls and restricts the information flow from the external interfaces to the network controller (which covers the information flow to and from the internal network).

The TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax etc) or system administration functions via the Web User Interface (Web UI) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the Web User Interface or the Local User Interface. The password will be obscured[2] as it is being entered. The TOE provides for user identification and authorization as configured by the system administrator.

The TOE restricts (normal) users' access to the documents. A user can only access his/her own documents.

The TOE can integrate with an IPv4 or IPv6 network with native support for dhcp/dhcpv6.

[2] The LUI obscures input with the asterisk character. The specific character used to obscure input at the WebUI is browser dependent.

The TOE supports the Common Access Card (CAC) standard and other methods (refer to chapter 1.3.2.3) for remote authentication.

1.2.2. TOE Type

The TOE is a multi-function device (MFD) that provides copy and print (monochrome and color), document scanning (monochrome and color) and optional FAX services.

1.2.3. Required Non-TOE Hardware, Software and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function device, however, the network security and fax flow features are only useful in environments where the TOE is connected to a network or PSTN. TSF_NET_ID is only available when one of the following remote authentication services is present on the network that the TOE is connected to: LDAP or Kerberos. CAC based TSF_NET_ID requires CAC compliant smart cards and smart card readers.

1.3. TOE Description

This section provides context for the TOE evaluation by identifying the logical and physical scope of the TOE, as well as its evaluated configuration.

1.3.1. Physical Scope of the TOE

The TOE is a Multi-Function Device (Xerox WorkCentre™ 7525/7530/7535/7545/7556) that consists of a printer, copier, scanner, FAX (when purchased by the consumer), and email, as well as all Administrator and User guidance. The difference between the models is their printing speed. The hardware included in the TOE is shown in Figure 2 above. The optional FAX card is not shown in this figure[3].

The various software and firmware ("Software") that comprise the TOE are listed in Table 2. A system administrator can ensure that they have a TOE by printing a configuration sheet and comparing the version numbers reported on the sheet to the table below.

[3] For installation, the optional FAX card must be fitted into the machine. After powering on the machine, the Fax Install window pops up on the Local UI with step by step instructions for installation.

Table 2: Evaluated Software/Firmware version

Software/Firmware Item	WorkCentre 7525/7530/7535/7545/7556
System Software	061.121.221.28308
Network Controller Software	061.121.25025
User Interface Software	061.121.24120
Marking Engine Software (Options)	
- WC 7525/7530/7535	081.077.000
- WC 7545/7556	082.077.000
Copy Controller Software	061.121.24121
Document Feeder Software (DADH)	007.008.050
Finisher Software (Options)	
- A-Finisher	013.000.000
- C-Finisher	032.042.000
- SB-Finisher	005.009.000
Fax Software	003.010.004
Scanner Software	030.141.115

NOTE: For the remainder of this Security Target, the terms "Network Controller" and "Copy Controller" will refer to the "Network Controller" and "Copy Controller" software components of the "Controller" subsystem.

A customer of the TOE can determine whether the Xerox Embedded Fax accessory, Xerox Workflow Scan accessory and Image Overwrite Security Package[4] are installed by reviewing the TOE configuration report. A consumer of the TOE can also determine that they have the evaluated version of the TOE by reviewing the TOE configuration report and comparing the version numbers to the content of Table 2, above.

The Administrator and User guidance included in the TOE are listed in Table 3. A system administrator or user can ensure that they have the appropriate

[4] Xerox Embedded Fax accessory, Xerox Workflow Scan accessory and Image Overwrite Security Package are a part of the Network Controller or Copy Controller software package and do not have individual version identifiers.

guidance by comparing the software version number to the version numbers listed in the table below.

Table 3: System User and Administrator Guidance

Title	Document Number	Date
Xerox® WorkCentre® 7500 Series System Administrator Guide v1.0	None	September 2010
Xerox® WorkCentre® 7500 Series User Guide v1.0	None	September 2010
Secure Installation and Operation of Your WorkCentre™ 7525/7530/7535/7545/7556 v1.3	None	December 2011

The TOE's physical interfaces include a power port, an Ethernet port, USB ports, serial ports, FAX ports (if the optional FAX card is installed), Local User Interface (LUI) with keypad, a document scanner, a document feeder and a document output.

1.3.2. Logical Scope of the TOE

The logical scope of the TOE includes all software and firmware that are installed on the product (see Table 2). The TOE logical boundary is composed of the security functions provided by the product.

The following security functions are controlled by the TOE:

- Image Overwrite (TSF_IOW)
- Authentication (TSF_ AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU)
- Cryptographic Operations (TSF_FCS)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Network Security (TSF_NET_SEC)
- Information Flow Security (TSF_ FLOW)
- Security Management (TSF_FMT)
- User Data Protection – Disk Encryption (TSF_FDP_UDE)

1.3.2.1. Image Overwrite (TSF_IOW)

The TOE has an "Immediate Image Overwrite" (IIO) function that overwrites files created during job processing. This IIO process automatically starts for all abnormally terminated copy, print, scan or fax jobs stored on the HDD prior to coming "on line" when any of the following occurs: a reboot or once the MFD is turned back on after a power failure/unorderly shutdown.

The TOE also has an "On-Demand Image Overwrite" (ODIO) function that overwrites the hard drive(s) *on-demand* of the system administrator. The

ODIO function operates in two modes: full ODIO and standard ODIO. A standard ODIO overwrites all files written to temporary storage areas of the HDD. A full ODIO overwrites those files as well as the Fax mailbox/dial directory and Scan-to-mailbox data.

Contents stored on the hard disk are overwritten using a three pass overwrite procedure.

1.3.2.2. Authentication (TSF_AUT)

A user must authenticate by entering a username and password prior to being granted access to the Local UI or the Web UI. While the user is typing the password, the TOE obscures[5] each character entered.

Upon successful authentication, users are granted access based on their role and predefined privileges. Only a system administrator is allowed full access to the TOE including all the system administration functions. Each common user's access is determined by which function (copy, scan, print, fax etc.) they have permission for.

If configured for local authentication the system requires the system administrator to enter a username and password for each user. The system will authenticate the user against an internal database.

By default, the Local UI will terminate any session that has been inactive for 1 minutes. By default, the Web UI will terminate any session that has been inactive for 60 minutes. The system administrator can configure both the Local UI and Web UI session timeouts to terminate an inactive session after some other period of time.

1.3.2.3. Network Identification (TSF_NET_ID)

As an alternative to TSF_AUT, the TOE allows user name and password for a user to be validated by a designated authentication server (a trusted remote IT entity). The user is not required to login to the network; account information entered at Local UI or Web UI of the TOE is authenticated at the server instead of the TOE. The remote authentication services[6] supported by the TOE include: CAC authentication, LDAP v4, Kerberos v5 (Solaris) and Kerberos v5 (Windows 2000/2003).

The TOE maintains the username from a successful authentication during the context of the job, and this value is entered into the audit log as the *user name*.

---

[5] The LUI obscures input with the asterisk character. The specific character used to obscure input at the WebUI is browser dependent

[6] User account (authorization privilege) information can be maintained locally by the TOE or at the remote authentication server without impacting how a user session is presented or controlled; however, the use of remote authentication servers for this purpose is outside the scope of this evaluation.

1.3.2.4. Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., copy/print/scan/fax job completion) to identified users. The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported for viewing and analysis. The downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

1.3.2.5. Cryptographic Operations (TSF_FCS)

The TOE utilizes digital signature generation and verification (RSA), data encryption (TDES, AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) to support secure communication between the TOE and remote trusted products. Those packages meet the following standards: 3DES – FIPS 46-3 (cert #826 and cert # 1174); AES - FIPS 197 (cert #1131 and cert# 1821); SHA-1, SHA-256 – FIPS 180-3 (cert # 1599), HMAC - FIPS 198 (cert #644 and cert # 1076); RSA - FIPS 186-3 (cert # 914).

1.3.2.6. User Data Protection – Disk Encryption (TSF_FDP_UDE)

The TOE utilizes data encryption (AES) to support encryption and decryption of designated portions of the hard disk where user files may be temporarily stored. The algorithm deployed meets the following standard: AES-FIPS-197 (CAVP Certificate No. 1131).

1.3.2.7. User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is generated by the system administrator specifying a series of rules to “accept,” “deny,” or “drop” packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. The IP Filter supports the construction of IPv4 filtering policies. Additionally, rules can be generated specifying filtering options based on port number given in the received packet. IP Filtering is not available for IPv6; however, the effect of IP Filtering can be accomplished for IPv6 by configuring IPSec associations.

1.3.2.8. Network Security (TSF_NET_SEC)

The TOE supports various secure communication protocols as part of its security solution. These includes: SSL for Web UI; SSL for document transfers to the remote file depository; IPSec for communication over IPv4 and IPv6; and Kerberos or SSL for remote authentication.

1.3.2.9. Information Flow Security (TSF_FLOW)

The TOE controls and restricts the data/information flow from the Local User Interface (LUI), document scanner and document feeder to the network controller (which covers the information flow to and from the internal network). All data and/or commands received from these interfaces are processed and in most cases transformed by the copy controller before submitted to the network controller. The network controller further processes the data before sending them to the internal network.

The TOE controls and restricts the information flow between the PSTN port of the optional FAX board (if installed) and the network controller. Commands cannot be sent to the internal network via the PSTN. Data received are processed before admitted to the internal network. A direct connection from the internal network to external entities by using the telephone line of the TOE is also denied.

If the optional FAX board is not installed, an information flow from or to the FAX port is not possible at all.

1.3.2.10. Security Management (TSF_FMT)

Only authenticated system administrators can enable or disable the Immediate Image Overwrite function, change the system administrator password, start an On Demand Image Overwrite operation or perform other administrative functions.

While IIO can be disabled, doing so will remove the TOE from its evaluated configuration.

User's access to the TOE functions, Job or Image Data stored inside the TOE is restricted, in accordance with the applicable TOE Security Policies.

The TOE is capable of verifying the integrity of the TSF at the request of the administrator.

1.4.Evaluated Configuration

In its evaluated configuration, IIO and ODIO (the Image Overwrite Security Package) are installed and enabled on the TOE; SSL is enabled on the TOE; and User Authorization is enabled on the TOE. The FAX (Xerox Embedded Fax accessory) option, if purchased by the consumer, is installed and enabled on the TOE. The LanFax option is included in the evaluated configuration of the TOE. IPX and AppleTalk network communication, USB Direct Printing and Internet Fax are not included in the evaluated configuration of the TOE.

In its evaluated configuration, the following options should be disabled:

- Network Accounting
- Copy/Print, Store and Reprint

- SMart eSolutions
- Xerox Extensible Interface Platform (EIP)

Please see http://www.xerox.com/information-security/product/enus.html for more specific information about maintaining the security of this TOE.

2. CONFORMANCE CLAIMS

This section describes the conformance claims of this Security Target.

2.1.Common Criteria Conformance Claims

The Security Target is based upon:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 3, CCMB-2009-07-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 3, CCMB-2009-07-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- Part 2 extended
- Part 3 conformant
- Evaluation Assurance Level (EAL) 2+

2.2.Protection Profile Claims

This Security Target claims demonstrable conformance to the "*IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ -2008 Operational Environment B (IEEE Std. 2600.2-2009)*" Protection Profile dated 26 February 2010 (IEEE 2600.2™-2009).

2.3.Package Claims

This Security Target claims conformance to the EAL2 package augmented with ALC_FLR.3, and the following additional packages from the "*IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ -2008 Operational Environment B (IEEE Std. 2600.2-2009)*" Protection Profile dated 26 February 2010:

- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B

- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
- 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment B
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

2.4.Rationale

The TOE type in this ST (multifunction or hardcopy device) is the same as the TOE type for IEEE 2600.2.

The Security Problem Definition (Threats, Assumptions and Organizational Security Policies) and Objectives have been copied directly from IEEE Std. 2600.2-2009 and have not been modified. One security objective for the TOE (O.AUDIT_STORAGE.PROTECTED) has been added in accordance to application notes 7 from IEEE Std. 2600.2-2009. One security objective for the IT environment (OE.USER.AUTHENTICATED) has been added in accordance to application notes 37, 42 and 43 from IEEE Std. 2600.2-2009. The statement of Security Requirements contains the SFRs from IEEE Std. 2600.2-2009 as well as additional SFRs that are taken from CC Part 2. By including all of the SFRs from IEEE Std. 2600.2-2009 and including additional SFRs (none of which conflict with each other), the statement of Security Requirements is necessarily at least as strict as the statement in IEEE Std. 2600.2-2009, if not more strict. The rationales for objectives, threats, assumptions, organizational security policies and security requirements have been copied from IEEE Std. 2600.2-2009 and have been augmented to address the requirements that have been added from CC Part 2.

The IEEE Std. 2600.2-2009 statement of Common Security Functional Requirements has been augmented with additional (including iterated) SFRs from CC Part 2:

Family	Augmentation
Audit	FAU_STG.1, FAU_STG.4
Cryptographic Support	FCS_COP.1
Identification and Authentication	FIA_UAU.7

The following packages from IEEE Std. 2600.2-2009 have been augmented with additional (including iterated) SFRs from CC Part 2:

Package	Augmentation
PRT	
SCN	
CPY	
FAX	
DSR	
SMI	FDP_IFC.1 (FILTER), FDP_IFF.1 (FILTER)

3. SECURITY PROBLEM DEFINITION

The Security Problem Definition describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

3.1.Definitions

3.1.1. 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
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). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

3.1.2. Objects (Assets)

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

3.1.2.1. 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 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.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

3.1.2.2. TSF Data

TSF Data is data created by and for the TOE and might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data. The TSF Data assets for this TOE has been categorized according to whether they require protection from unauthorized alteration (TSF Protected Data) or protection from both unauthorized disclosure and unauthorized alteration (TSF Confidential Data). The data assets have been identified and categorized in Table 6: TSF Data and Table 7: TSF Data Categorization below.

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.

Table 7: TSF Data Categorization

TSF Protected Data	TSF Confidential Data
Configuration data	Audit Log
Device and network status information and configuration settings	Cryptographic keys
Device service and diagnostic data	X.509 Certificate (SSL)
	User IDs and Passwords
	User Access Permissions
	802.1x Credentials and Configuration
	IP filter table (rules)
	Email Addresses for fax forwarding

Application Note: IEEE Std. 2600.2-2009 defines *D.PROT* and *D.CONF*, and requires the ST author to categorize all TSF data as one of these two types: *data that should be protected, but does not affect the operational security of the TOE if it is disclosed (D.PROT), and data that does affect the operational security of the TOE if it is disclosed (D.CONF).*

3.1.2.3. Functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. These functions are used by SFR packages, and are identified and defined in the table below.

Table 8: SFR Package Functions for IEEE Std. 2600.2-2009

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.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

3.1.3. Operations

Operations are a specific type of action performed by a Subject on an Object. In this Security Target, five types of operations are considered: 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).

3.1.4. Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE. In this Security Target, four types of Channels are allowed:

Private Medium Interface: mechanisms for exchanging information that use (1) wired or wireless 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.

Shared-medium Interface: mechanisms for exchanging information that use wired or wireless network or non-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.

Original Document Handler: mechanisms for transferring User Document Data into the TOE in hardcopy form. It is an input channel.

Hardcopy Output Handler: mechanisms for transferring User Document Data out of the TOE in hardcopy form. It is an output channel.

In practice, at least one input channel and one output channel would be present in any HCD configuration, and at least one of those channels would be either an Original Document Handler or a Hardcopy Output Handler.

3.2. Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Security Target are based on the condition that all of the assumptions described in this section are satisfied.

Table 9: Assumptions for the TOE

Assumption	Definition
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.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.
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.

3.3. Threats

3.3.1. Threats Addressed by the TOE

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Security Target address the threats posed by these threat agents.

This section describes threats to assets described in Section 3.1.2.

Table 10: Threats to User Data for the TOE

Threat	Affected Asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 11: Threats to TSF Data for the TOE

Threat	Affected Asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.3.2. Threats Addressed by the IT Environment

There are no threats addressed by the IT Environment.

3.4. Organizational 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 12: Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF
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 external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment

4. SECURITY OBJECTIVES

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1.Security Objectives for the TOE

This section describes the security objectives that the TOE shall fulfill.

Table 13: Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
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.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that internal audit records are protected from unauthorized access, deletion and modifications.

4.2.Security Objectives for the Operational Environment

This section describes the security objectives that must be fulfilled by IT methods in the IT environment of the TOE.

Table 14: Security Objectives for the IT Environment

Objective	Definition
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.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 accessed in order to detect potential security violations, and only by authorized persons
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
OE.USER.AUTHENTICATED	The IT environment shall provide support for user identification and authentication and protect the user credentials in transit when TOE operates in remote identification and authentication mode.

4.3.Security Objectives for the Non-IT Environment

This section describes the security objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

Table 15: Security Objectives for the Non-IT Environment

Objective	Definition
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.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.
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.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4.Rationale for Security Objectives

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 16: Completeness of Security Objectives

	Objectives																				
Threats. Policies, and Assumptions	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	OE.INTERFACE.MANAGED	OE.USER.AUTHENTICATED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	X						X	X								X					
T.DOC.ALT		X					X	X								X					
T.FUNC.ALT			X				X	X								X					
T.PROT.ALT				X			X	X								X					
T.CONF.DIS					X		X	X								X					
T.CONF.ALT						X	X	X								X					
P.USER.AUTHORIZATION							X	X								X					
P.SOFTWARE.VERIFICATION									X												
P.AUDIT.LOGGING										X	X	X	X	X							
P.INTERFACE.MANAGEMENT															X			X			
A.ACCESS.MANAGED																	X				
A.ADMIN.TRAINING																			X		
A.ADMIN.TRUST																				X	
A.USER.TRAINING																					X

Table 17: Sufficiency of Security Objectives

Threats. Policies, and Assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.DOC.ALT	User Document Data may be altered by unauthorized persons	O.DOC.NO_ALT protects D.DOC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.FUNC.ALT	User Function Data may be altered by unauthorized persons	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons	O.PROT.NO_ALT protects D.PROT from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the

Threats. Policies, and Assumptions	Summary	Objectives and rationale
		basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons	O.CONF.NO_ALT protects D.CONF from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
		OE.USER.AUTHENTICATED establishes alternative (remote) means for user identification and authentication as the basis for authorization to use the TOE
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		O.AUDIT_STORAGE.PROTECTED protects internal audit records from unauthorized access, deletion and modifications
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modifications
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies

Threats. Policies, and Assumptions	Summary	Objectives and rationale
	and its IT environment.	OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE
A.ADMIN.TRAINING	Administrators are aware of and trained to follow security policies and procedures	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	TOE Users are aware of and trained to follow security policies and procedures	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5. EXTENDED COMPONENTS DEFINTION

This Security Target defines components that are extensions to Common Criteria 3.1 Release 3, Part 2.

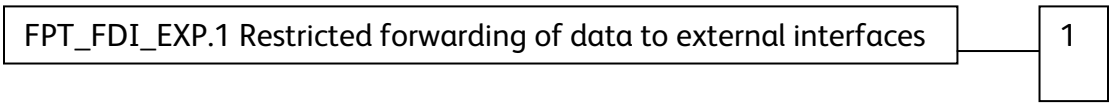
5.1.FPT_FDI_EXP Restricted forwarding of data to external interfaces

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 this data is 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:

a) 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 is 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 Security Target, 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 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 could therefore be placed in either the FDP or 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 lead 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*].

6. SECURITY REQUIREMENTS

This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1.Conventions

All operations performed on the Security Functional Requirements or the Security Assurance Requirements need to be identified. For this purpose the following conventions shall be used.

- Assignments will be written in [normal text with brackets]
- Selections will be written in *underlined and italic text*.
- Refinements will be written **bold**
- Iterations will be performed on components and functional elements. The component ID defined by the Common Criteria (e.g. FDP_IFC.1) will be extended by an ID for the iteration (e.g. “(FILTER)”). The resulting component ID would be “FDP_IFC.1 (FILTER)”.
- Where an iteration is identified in rationale discussion as “all”, the statement applies to all iterations of the requirement (e.g. “FMT_MTD.1 (all)”)
- SFRs and TSPs that appear in the IEEE 2600.2 are marked as such; all unmarked SFRs have been added to this ST from CC Part 2.

6.2. TOE Security Policies

This chapter contains the definition of security policies which must be enforced by the TSF.

6.2.1. IP Filter SFP (TSP_FILTER)

The security function "User Data Protection -- IP Filtering" (TSF_FDP_FILTER) requires that network traffic to and from the TOE will be filtered in accordance with the rules defined by the system administrator at the Web User Interface configuration editor for IP Filtering. This policy will be enforced on:

- SUBJECTS: External entities that send network traffic to the TOE.
- INFORMATION: All IP-based traffic to and from that destination.
- OPERATIONS: Pass network traffic.

Note: The TOE cannot enforce the IP Filtering (TSP_FILTER) when it is configured for IPv6.

6.2.2. User Access Control SFP (UAC_SFP) (IEEE Std. 2600.2-2009)

The Security Function Policy (SFP) described in Table 18: User Access Control SFP is referenced by the Class FDP SFRs.

Table 18: User Access Control SFP

Object	Attribute	Operation(s)	Subject	Access Control Rule
D.DOC	+PRT	Read	U.NORMAL	Denied, except for his/her own documents
			U.ADMINISTRATOR	Denied, except for his/her own documents
		Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except when the associated D.FUNC is deleted.
	+SCN	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+CPY	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+FAXIN	Read, Delete	U.ADMINISTRATOR	Allowed
		Read, Delete	U.NORMAL	Denied
	+FAXOUT	Read, Delete	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents
	+DSR and +SCN	Read, Delete	U.NORMAL	Denied, except for his/her own documents
			U.ADMINISTRATOR	Allowed
D.FUNC	Any Attribute, except +CPY	Modify	U.NORMAL, U.ADMINISTRATOR	Denied
	+PRT	Delete	U.NORMAL	Denied, except for his/her own documents
			U.ADMINISTRATOR	Allowed
	+SCN	Delete	U.NORMAL, U.ADMINISTRATOR	Denied
	+CPY	Delete, Modify	U.NORMAL, U.ADMINISTRATOR	Denied, except for his/her own documents

	+FAXIN	Delete	U.NORMAL, U.ADMINISTRATOR	Denied
	+FAXOUT	Delete	U.NORMAL	Denied
	+FAXOUT	Delete	U.ADMINISTRATOR	Allowed

Table 19: Attributes Definition

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

Application Note: IEEE Std. 2600.2-2009 specifies the contents of FDP_ACC.1 for each function package that is claimed by a ST and a Common Access Control SFP for D.FUNC and D.DOC (Operation: read). In this ST, the SFPs for each package are combined with the Common Access Control SFP then refined to form Table 18 (User Access Control SFP). User Access Control SFP represents more detail and a more restrictive requirement than the combination of package SFPs and the Common Access Control SFP. Hence the ST is conformant to IEEE Std. 2600.2-2009.

Application Note: A document (D.DOC) is "owned" by a User (U.User) if that document was created or submitted to the TOE by that User. The only exception are documents received as fax (D.DOC +FAXIN), for which the system administrators are considered as the owner. This is in conformance to IEEE Std. 2600.2-2009 application note 94 and 95.

Application Note: Access control rules for the "Create" Operation are not specified because typically, any authorized U.User can create his/her own documents and cannot create documents that are owned by another User.

Application Note: IEEE Std. 2600.2-2009 (table 23) defined attribute +DSR does not apply to D.FUNC, and in this ST is only applicable to D.DOC with attribute +SCN. Attribute +SMI does not apply to this SFP.

6.2.3. TOE Function Access Control SFP (TF_SFP) (IEEE Std. 2600.2-2009)

Users (U.NORMAL) require explicit authorization from system administrators (U.ADMINISTRATOR) for them to be allowed to perform the following TOE Functions as defined in the IEEE Std. 2600.2-2009 SFR Packages in Section 12.3 via the Web UI or the LUI:

- Print (PRT)

- Scan (SCN)
- Fax (FAX)
- Copy (CPY)
- Document Storage and Retrieval (DSR)
- Transmit data via Shared-medium Interfaces (SMI)

Any User who is authorized to establish an connection with the TOE through the Ethernet port is allowed to perform the following TOE Functions as defined in the IEEE Std. 2600.2-2009 SFR Packages in Section 12.3:

- Print (PRT)
- Fax (FAX) – LanFax only
- Transmit data via Shared-medium Interfaces (SMI)

6.3.Security Functional Requirements

The TOE satisfies the SFRs delineated in Table 20: TOE Security Functional Requirements. The rest of this section contains a description of each component and any related dependencies.

Table 20: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF Testing
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel

6.3.1. Class FAU: Security audit

6.3.1.1. FAU_GEN.1 Audit data generation (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

— Start-up and shutdown of the audit functions;

— All auditable events for the *not specified* level of audit; and

[all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 21].

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

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

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 21: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required),

— And the following audit attribute:

- Entry number (an integer value from 1 to the number of entries in the audit log)]

Table 21: Audit Data Requirements

Auditable Event	Relevant SFR	Audit Level	Additional Information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Changes to the time	FPT_STM.1	Minimum	None required
Failure of the trusted channel functions[7]	FTP_ITC.1	Minimum	Non required

6.3.1.2. FAU_GEN.2 User identity association (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

6.3.1.3. FAU_STG.1 Protected audit trail storage

Hierarchical to: None.

Dependencies: FAU_GEN.1 Audit data generation

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

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

6.3.1.4. FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3.

Dependencies: FAU_STG.1 Protected audit trail storage

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

[7] This audit event is required by the addition of the IEEE 2600.2-SMI SFR Package. The developer added it to the existing table of events rather than adding an iteration for FAU_GEN.1.

6.3.2. Class FCO: Communication

There are no Class FCO security functional requirements for this Security Target.

6.3.3. Class FCS: Cryptographic support

6.3.3.1. FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [the cryptographic operations listed in the Cryptographic Operations column of Table 22] in accordance with a specified cryptographic algorithm [the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 22] and cryptographic key sizes [the cryptographic key sizes listed in the Key Sizes (bits) column of Table 22] that meet the following: [the list of standards in the Standards (Certificate #) column of Table 22].

Table 22: Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple DES (CBC)	168	FIPS 46-3 (cert #826 and cert # 1174)
	AES (CBC)	256	FIPS 197 (cert #1131 and cert# 1821)
Digital Signature Generation and Verification	RSA	1024	FIPS 186-3 (cert # 914)
Message Digest	SHA-1, SHA-256	N/A	FIPS 180-3 (cert # 1599)
Message Authentication	HMAC	160	FIPS 198 (cert #644 and cert # 1076)

6.3.4. Class FDP: User data protection

6.3.4.1. FDP_ACC.1 (USER) Subset access control (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 18] on [the list of users as subjects, objects, and operations among subjects and objects covered by the User Access Control SFP in Table 18].

Application Note: This SFR covers FDP_ACC.1 (a) and FDP_ACC.1 from all claimed packages (PRT, SCN, CPY, FAX, DSR) in the IEEE Std. 2600.2 PP.

6.3.4.2. FDP_ACC.1 (FUNC) Subset access control (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] on [users as subjects, TOE functions as objects, and the right to use the functions as operations].

Application Note: This SFR is FDP_ACC.1 (b) from The IEEE Std. 2600.2 PP.

6.3.4.3. FDP_ACF.1 (USER) Security attribute based access control (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 18] to objects based on the following: [the list of users as subjects and objects controlled under the User Access Control SFP in Table 18, and for each, the indicated security attributes in Table 18].

FDP_ACF.1.2 (USER) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules specified in the User Access Control SFP in Table 18 governing access among controlled users as subjects and

controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 (USER) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (USER) The TSF shall explicitly deny access of subjects to objects based on the [none].

Application Note: This SFR covers FDP_ACF.1 (a) and FDP_ACF.1 from all claimed packages (PRT, SCN, CPY, FAX, DSR) in the IEEE Std. 2600.2 PP.

6.3.4.4. FDP_ACF.1 (FUNC) Security attribute based access control (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] to objects based on the following: [users, roles and their individual permissions to perform any or all of the following functions: print, scan, copy, fax, document storage and retrieval, access to shared-medium interface].

FDP_ACF.1.2 (FUNC) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the user who is explicitly authorized by U.ADMINISTATOR to use a function is allowed to access the function via Web UI or LUI].

FDP_ACF.1.3 (FUNC) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

- the user acts in the role U.ADMINISTRATOR is allowed to access all functions available;
- all users authorized for remote connection to the TOE are allowed to access print, LanFax, and access to shared-medium interface].

FDP_ACF.1.4 (FUNC) The TSF shall explicitly deny access of subjects to objects based on the [none].

Application Note: This SFR is FDP_ACF.1 (b) from The IEEE Std. 2600.2 PP.

6.3.4.5. FDP_IFC.1 (FILTER) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (FILTER) The TSF shall enforce the [IPFilter SFP] on [

- Subjects: External entities that send traffic to the TOE;
- Information: All IP-based traffic to/from that source/destination;
- Operations: send or receive network traffic].

6.3.4.6. FDP_IFF.1 (FILTER) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization.

FDP_IFF.1.1 (FILTER) The TSF shall enforce the [IPFilter SFP] based on the following types of subject and information security attributes: [

- Subjects: External entities that send traffic to the TOE
  - IP address,
- Information: IP Packet
  - Source IP address, protocol used (TCP or UDP), destination TCP or UDP port].

FDP_IFF.1.2 (FILTER) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- The source IP address matches a rule in the TOE's rule base
- If configured, the destination transport layer port matches a rule in the TOE's rule base.]

FDP_IFF.1.3 (FILTER) The TSF shall enforce the [implicit allow if no rules have been defined].

FDP_IFF.1.4 (FILTER) The TSF shall explicitly authorize an information flow based on the following rules: [if the rule is the default all].

FDP_IFF.1.5 (FILTER) The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes or if a rule explicitly denies an information flow].

Application Note: When custom rules have not been defined by the system administrator, the default rule (allow all traffic) will apply. Because it is a wildcard rule, all IP addresses, ports and protocols (either TCP or UDP) will be a match for allowed traffic.

6.3.4.7. FDP_RIP.1 Subset residual information protection (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	No dependencies
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].

6.3.5. Class FIA: Identification and authentication

6.3.5.1. FIA_ATD.1 User attribute definition (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [username, password, role, list of objects and functions that the user has permission to access].

6.3.5.2. FIA_UAU.1 Timing of authentication (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [printing or LanFax requests received via printing protocols] 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.

6.3.5.3. FIA_UAU.7 Protected authentication feedback

Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of Authentication

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

6.3.5.4. FIA_UID.1 Timing of identification (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_UID.1.1	The TSF shall allow [printing or LanFax requests received via printing protocols] 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.

6.3.5.5. FIA_USB.1 User-subject binding (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [identity, list of objects and functions that the user has permission to access].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [subjects will be assigned the security attributes of the user that they are acting on behalf of].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [security attributes of subjects acting on behalf of a user will not be changed while an action is in progress and cannot be changed by anyone but U.ADMINISTRATOR].

6.3.6. Class FMT: Security management

6.3.6.1. FMT_MSA.1 (USER) Management of security attributes (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 18] to restrict the ability to *change_default, modify, delete, [read]* the security attributes [all] to [U.ADMINISTRATOR].

Application Note: This SFR is FMT_MSA.1 (a) from The IEEE Std. 2600.2 PP.

6.3.6.2. FMT_MSA.1 (FUNC) Management of security attributes (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (FUNC) The TSF shall enforce the [TOE Function Access Control SFP] to restrict the ability to *change_default, modify, delete, [read]* the security attributes [user access permissions] to [U.ADMINISTRATOR].

Application Note: This SFR is FMT_MSA.1 (b) from The IEEE Std. 2600.2 PP.

6.3.6.3. FMT_MSA.3 (USER) Static attribute initialisation (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (USER) The TSF shall enforce the [User Access Control SFP in Table 18] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (USER) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

Application Note: This SFR is FMT_MSA.3 (a) from The IEEE Std. 2600.2 PP.

6.3.6.4. FMT_MSA.3 (FUNC) Static attribute initialisation (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 (FUNC) The TSF shall enforce the [TOE Function Access Control Policy] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (FUNC) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

Application Note: This SFR is FMT_MSA.3 (b) from The IEEE Std. 2600.2 PP.

6.3.6.5. FMT_MTD.1 (MGMT1) Management of TSF data (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (MGMT1) The TSF shall restrict the ability to *[download]* the [audit log] to [U.ADMINISTRATOR].

Application Note: This SFR is part of FMT_MTD.1 from The IEEE Std. 2600.2 PP.

6.3.6.6. FMT_MTD.1 (MGMT2) Management of TSF data (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 (MGMT2) The TSF shall restrict the ability to *change_default, modify, delete, [read]* the [*access permissions of U.NORMAL*] to [U.ADMINISTRATOR].

Application Note: FMT_MTD.1 (MGMT1) and FMT_MTD.1 (MGMT2) appear as a single requirement in IEEE P2600.2. Because the Common Criteria does not allow for iterating elements, this Security Target has iterated the entire requirement for correctness.

Application Note: This SFR is part of FMT_MTD.1 from The IEEE Std. 2600.2 PP.

6.3.6.7. FMT_MTD.1 (KEY) Management of TSF data (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FMT_MTD.1.1 (KEY)	The TSF shall restrict the ability to *modify, delete, [create]* the [• IPSec Secret Key, • X.509 Server certificate] to [U.ADMINISTRATOR].

6.3.6.8. FMT_MTD.1 (FILTER) Management of TSF data (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FMT_MTD.1.1 (FILTER)	The TSF shall restrict the ability to *modify*, *delete*, *[create*, *read]* the [• IP filter rules • Fax Forwarding Email Addresses] to [U.ADMINISTRATOR].

6.3.6.9. FMT_SMF.1 Specification of Management Functions (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [

- Enable/disable Immediate Image Overwrite (IIO) [TSF_IOW];
- Create and Delete User (ID);
- Enable/disable and configure Common Access Card use;
- Configure USB ports;
- Change System Administrator Password;
- Set and Change User Local Authentication Password;
- Invoke ODIO [TSF_IOW];
- Create a recurrence schedule for "On Demand" image overwrite;
- Enable/disable audit function;
- Transfer the audit records (if audit is enabled) to a remote trusted IT product;
- Enable/disable SSL;
- Create/upload/download X.509 certificates;
- Enable/disable and configure 802.1x;
- Enable/disable and configure IPSec;
- Enable/disable and configure SNMPv3;
- Configure (specify the IP address and/or IP address range, port and port range for remote trusted IT products (presumed) allowed to connect to the TOE via the network interface) IP filtering;
- Enable/disable Disk Encryption;
- Configure network authentication;
- Configure local device and service authorization;
- Configure WebUI and Local UI session timeout;
- Manage receive fax (job) pass codes;
- Enable/disable and configure fax forwarding to email; and,
- Perform Software Self-test].

6.3.6.10. FMT_SMR.1 Security roles (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [U.ADMINISTRATOR (System Administrator), U.NORMAL (Standard User), *Nobody*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated**.

Application Note: The role "Nobody" cannot be assigned to any user. It is included in FMT_SMR.1.1 only because it has been used as a role in other SFRs. IEEE Std. 2600.2 PP defines two roles *U.ADMINISTRATOR* and *U.NORMAL* which in the context of the TOE are equivalent to "System Administrator" and "Standard User[8]" respectively.

6.3.7. Class FPR: Privacy

There are no Class FPR security functional requirements for this Security Target.

6.3.8. Class FPT: Protection of the TSF

6.3.8.1. FPT_STM.1 Reliable time stamps (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.3.8.2. FPT_TST.1 TSF testing (IEEE Std. 2600.2-2009)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *at the conditions: [*

- *reboot, or*
- *once the device is turned on after a power failure/unorderly shutdown]*

to demonstrate the correct operation of [*the following parts of TSF: Immediate Image Overwrite*].

[8] Within Administrator and User guidance included in the TOE, the role "standard user" is often referred to as simply "user.

FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [*the following parts of TSF data:* • *Software Module version (configuration data);* • *IP Filtering Tables*].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

6.3.8.3. Class FRU: Resource utilization

There are no Class FRU security functional requirements for this Security Target.

6.3.9. Class FTA: TOE access

6.3.9.1. FTA_SSL.3 TSF-initiated termination (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [U.ADMINISTRATOR configurable amount of time in the Local UI or on the WebUI].

6.3.10. Class FTP: Trusted paths/channels

6.3.10.1. FTP_ITC.1 Inter-TSF trusted channel (IEEE Std. 2600.2-2009)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *the TSF, another 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].

6.4.Explicitly Stated Requirements for the TOE

6.4.1. FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces (IEEE Std. 2600.2-2009)

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 [any external Interface] from being forwarded without further processing by the TSF to [any Shared-medium Interface].

Application Note: IEEE 2600.2 PP Application Note 116 states the following: *"The ST Author can use this SFR to define the roles that are permitted to allow unmediated transmission between Interfaces. If unmediated transmission is never allowed, "Nobody" should be instantiated as the "authorized identified roles."* This extended component, as defined in IEEE 2600.2, does not provide a mechanism for specifying authorized identified roles. For this reason, the authorized identified role that is not included in this extended requirement claim should be "Nobody". Additionally, for this TOE, the restricted forwarding from the external interfaces to the network controller are architectural design features which cannot be configured; hence the dependencies on FMT_SMF.1 and FMT_SMR.1 are not met.

6.5. TOE Security Assurance Requirements

Table 23 lists the security assurance requirements for "IEEE 2600.2, *Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment B*", and related SFR packages, EAL2+ augmented with ALC_FLR.3. This Security Target claims conformance with these Security Assurance Requirements; they are not iterated or refined from their counterparts in CC Part 3.

Table 23: IEEE 2600.2 Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.3 Systematic flaw remediation (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.6.Rationale for Security Functional Requirements

Table 24: Completeness of Security Functional Requirements and Table 25: Sufficiency of Security Functional Requirements below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. These tables contain the original rationale from IEEE Std. 2600.2-2009. Rationales for the SFRs that have been added to this Security Target, that do not originate in IEEE Std. 2600.2-2009, have been added to these tables. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 24: Completeness of Security Functional Requirements

SFRs	Objectives										
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED
FAU_GEN.1										**P**	**P**
FAU_GEN.2										**P**	**P**
FAU_STG.1											**P**
FAU_STG.4											**P**
FCS_COP.1	S	S	S	S	S	S					
FDP_ACC.1 (USER)	**P**	**P**	**P**								
FDP_ACC.1 (FUNC)							**P**				
FDP_ACF.1 (USER)	S	S	S								
FDP_ACF.1 (FUNC)							S				
FDP_IFC.1 (FILTER)								**P**			
FDP_IFF.1 (FILTER)								S			
FDP_RIP.1	**P**										
FIA_ATD.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	S
FIA_USB.1							**P**				
FMT_MSA.1 (USER)	S	S	S								
FMT_MSA.1 (FUNC)							S				
FMT_MSA.3 (USER)	S	S	S								
FMT_MSA.3 (FUNC)							S				
FMT_MTD.1 (MGMT1)				**P**	**P**	**P**					
FMT_MTD.1 (MGMT2)				**P**	**P**	**P**					
FMT_MTD.1 (FILTER)				**P**	**P**	**P**					
FMT_MTD.1 (KEY)				**P**	**P**	**P**					
FMT_SMF.1	S	S	S	S	S	S				S	
FMT_SMR.1	S	S	S	S	S	S	S				
FPT_STM.1										S	S
FPT_TST.1									**P**		
FPT_FDI_EXP.1								**P**			

SFRs	Objectives										
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED
FTA_SSL.3							**P**	**P**			
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

Table 25: Sufficiency of Security Functional Requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT	Protection of User Data from unauthorized disclosure or alteration	**FDP_ACC.1(USER)**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1(USER)	Supports access control policy by providing access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MSA.1(USER)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(USER)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_RIP.1**	**Enforces protection by making residual data unavailable.**

Objectives	Description	SFRs	Purpose
O.CONF.NO_DIS, O.PROT.NO_ALT, O.CONF.NO_ALT	Protection of TSF Data from unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MTD.1(MGMT1) FMT_MTD.1(MGMT2) FMT_MTD.1 (KEY) FMT_MTD.1 (FILTER)	**Enforces protection by restricting access.**
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.USER.AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	**FDP_ACC.1(FUNC)**	**Enforces authorization by establishing an access control policy.**
		FDP_ACF.1(FUNC)	Supports access control policy by providing access control function.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_UAU.1	**Enforces authorization by requiring user authentication.**
		FIA_UAU.7	Supports authorization by protecting passwords.
		FIA_UID.1	**Enforces authorization by requiring user identification.**
		FIA_USB.1	**Enforces authorization by distinguishing subject security attributes associated with user roles.**
		FMT_MSA.1(FUNC)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(FUNC)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMR 1	Supports authorization by requiring security roles.
		FTA_SSL.3	**Enforces authorization by terminating inactive sessions.**
O.INTERFACE.MANAGED	Management of external interfaces	**FDP_IFC.1 (FILTER)**	**Enforces management of external interfaces by establishing an information flow policy for the network and fax interfaces**

Objectives	Description	SFRs	Purpose
		FDP_IFF.1 (FILTER)	Supports management of external interfaces by enforcing information flow rules on the network and fax interfaces
		FIA_UAU.1	**Enforces management of external interfaces by requiring user authentication.**
		FIA_UID.1	**Enforces management of external interfaces by requiring user identification.**
		FTA_SSL.3	**Enforces management of external interfaces by terminating inactive sessions.**
		FPT_FDI_EXP.1	**Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces.**
O.SOFTWARE.VERIFIED	Verification of software integrity	**FPT_TST.1**	**Enforces verification of software by requiring self tests.**
O.AUDIT.LOGGED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**
		FIA_UID.1	Supports audit policies by associating user identity with events.
		FMT_SMF.1	Supports audit policies by requiring functions to enable logging of relevant events.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.AUDIT_STORAGE.PROTECTED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**

Objectives	Description	SFRs	Purpose
		FAU_STG.1	**Enforces the audit policies by preventing unauthorized modification or deletion.**
		FAU_STG.4	**Enforces the audit policies by preventing loss of newer audit trail data.**
		FIA_UID.1	Supports audit policies by requiring user identification
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, O.CONF.NO_ALT	Protection of User and TSF Data from unauthorized disclosure or alteration	FCS_COP.1	Supports protection by providing cryptographic operations for secure communication and enforces disk encryption.
		FTP_ITC.1	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**

6.7. Rationale for Security Assurance Requirements

This Security Target has been developed Using the "*IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ -2008 Operational Environment B (IEEE Std. 2600.2-2009)" and related SFR packages, EAL2+ augmented with ALC_FLR.2*; which was created to describe Hardcopy Devices used in commercial information processing environments that require a moderate level of document security, network security, and security assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE. Agents have limited or no means of infiltrating the TOE with code to effect a change and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

While IEEE Std. 2600.2-2009 augments EAL2 with ALC_FLR.2, Flaw reporting procedures, this ST augments EAL2 with ALC_FLR.3, Systematic flaw remediation. ALC_FLR.3 is hierarchical to ALC_FLR.2 and encompasses all requirements of ALC_FLR.2 plus some additional requirements. ALC_FLR.3 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place and their inclusion is expected by the

consumers of this TOE, and that consumers of this TOE are automatically notified of flaws and changes to the TOE.

6.8. Rationale for Dependencies

6.8.1. Security Functional Requirement Dependencies

Table 26: SFR Dependencies Satisfied is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 26: SFR Dependencies Satisfied

Functional Component ID	Dependency (ies)	Satisfied
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1	Yes
	FIA_UID.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	No[9]
	FCS_CKM.4	No[10]
FDP_ACC.1(USER)	FDP_ACF.1	Yes, FDP_ACF.1(USER)
FDP_ACC.1(FUNC)	FDP_ACF.1	Yes, FDP_ACF.1(FUNC)
FDP_ACF.1(USER)	FDP_ACC.1	Yes, FDP_ACC.1(USER)
	FMT_MSA.3	Yes, FMT_MSA.3(USER)
FDP_ACF.1(FUNC)	FDP_ACC.1	Yes, FDP_ACC.1(FUNC)
	FMT_MSA.3	Yes, FMT_MSA.3 (FUNC)
FDP_IFC.1 (FILTER)	FDP_IFF.1	Yes, FDP_IFF.1 (FILTER)
FDP_IFF.1 (FILTER)	FDP_IFC.1	Yes, FDP_IFC.1 (FILTER)
	FMT_MSA.3	No[11]
FDP_RIP.1	None	
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.7	FIA_UAU.1	Yes
FIA_UID.1	None	
FIA_USB.1	FIA_ATD.1	Yes

[9] The dependency of FCS_COP.1 on FCS_CKM.1 and FCS_CKM.4 is not met because CCS Instruction #4, dated 28 July 2008, does not require that the FCS_CKM.1 and FCS_CKM.4 dependencies be met when just an algorithm but not the entire module is validated under the CMVP program.

[10] The dependency of FCS_COP.1 on FCS_CKM.1 and FCS_CKM.4 is not met because CCS Instruction #4, dated 28 July 2008, does not require that the FCS_CKM.1 and FCS_CKM.4 dependencies be met when just an algorithm but not the entire module is validated under the CMVP program.

[11] The dependency of FDP_IFF.1 (FILTER) on FMT_MSA.3 is not met because none of these functions support "a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values." (CC Part 2 Page 106). The TOE does not give system administrators the option of specifying default values, permissive or otherwise. In fact, these features are configured and, with the exception of IP Filter rules, cannot be modified by the system administrator other than to enable or disable them. It is for these reasons that the dependency on FMT_MSA.3 is not and cannot be expected to be met.

Functional Component ID	Dependency (ies)	Satisfied
FMT_MSA.1(USER)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (USER)
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1(FUNC)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (FUNC)
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.3(USER)	FMT_MSA.1	Yes, FMT_MSA.1(USER)
	FMT_SMR.1	Yes
FMT_MSA.3(FUNC)	FMT_MSA.1	Yes, FMT_MSA.1(FUNC)
	FMT_SMR.1	Yes
FMT_MTD.1(MGMT1)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1(MGMT2)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (FILTER)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (KEY)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	None	
FPT_TST.1	None	
FPT_FDI_EXP.1	FMT_SMF.1	No[12]
	FMT_SMR.1	No[13]
FTA_SSL.3	None	
FTP_ITC.1	None	

[12] For this TOE, the restricted forwarding from the external interfaces to the network controller are architectural design features which cannot be configured, hence the dependencies on FMT_SMF.1 is not met.

[13] For this TOE, the restricted forwarding from the external interfaces to the network controller are architectural design features which cannot be configured; hence the dependencies on FMT_SMF.1 and FMT_SMR.1 are not met.

6.8.2. Security Assurance Requirement Dependencies

SAR dependencies identified in the CC have been met by this ST as shown in Table 27.

Table 27: EAL2 (Augmented with ALC_FLR.3) SAR Dependencies Satisfied

Assurance Component ID	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	Yes, hierarchically Yes
ADV_FSP.2	ADV_TDS.1	Yes
ADV_TDS.1	ADV_FSP.2	Yes
AGD_OPE.1	ADV_FSP.1	Yes, hierarchically
AGD_PRE.1	None	
ALC_CMC.2	ALC_CMS.1	Yes, hierarchically
ALC_CMS.2	None	
ALC_DEL.1	None	
ALC_FLR.3	None	
ASE_CCL.1	ASE_ECD.1 ASE_INT.1 ASE_REQ.1	Yes Yes Yes, hierarchically
ASE_ECD.1	None	
ASE_INT.1	None	
ASE_OBJ.2	ASE_SPD.1	Yes
ASE_REQ.2	ASE_ECD.1 ASE_OBJ.2	Yes Yes
ASE_SPD.1	None	
ASE_TSS.1	ADV_FSP.1 ASE_INT.1 ASE_REQ.1	Yes, hierarchically Yes Yes, hierarchically
ATE_COV.1	ADV_FSP.2 ATE_FUN.1	Yes Yes
ATE_FUN.1	ATE_COV.1	Yes
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes Yes Yes Yes Yes
AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	Yes Yes Yes Yes Yes

7. TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE.

7.1. TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Sections 6.3 and 6.4. For reference, the TOE architecture is depicted in Figure 1.

- Image Overwrite (TSF_IOW)
- Information Flow Security (TSF_FLOW)
- System Authentication (TSF_AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Network Security (TSF_NET_SEC)
- Security Management (TSF_FMT)
- User Data Protection - Disk Encryption (TSF_FDP_UDE)

7.1.1. Image Overwrite (TSF_IOW)

FDP_RIP.1

The TOE implements an image overwrite security function to overwrite all temporary files created during processing of jobs, files (images) of completed or deleted jobs or any files that are deleted[14].

The controller spools and processes documents to be printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. The definition of this reserved section is statically stored within the TOE and cannot be manipulated. Immediately after the job has completed, the files are overwritten, and this is called Immediate Image Overwrite (IIO).

The TOE automatically starts an IIO procedure for all abnormally terminated copy, print, scan or fax jobs stored on the HDD prior to coming “on line” when any of the following

[14] Files are stored inside mailboxes. They may be deleted by their owner through individual file deletions or deletion of the mailbox.

occurs: a reboot or once the MFD is turned back on after a power failure/unorderly shutdown.

The image overwrite security function can also be invoked manually (on demand) by the system administrator (ODIO). Once invoked, the ODIO cancels all print and scan jobs, halts the printer interface (network), performs the overwrites, and then the network controller reboots. A scheduling function allows ODIO to be executed on a recurring basis as set up by the System Administrator.

A standard On Demand Image Overwrite (ODIO) overwrites all files written to temporary storage areas of the HDD. A full ODIO overwrites those files as well as the Fax mailbox/dial directory and Scan to mailbox data.

An ODIO cannot be aborted from either the WebUI or Local UI.

TSF_IOW overwrites the contents of the reserved section on the hard disk using a three pass overwrite procedure.

7.1.2. Information Flow Security (TSF_FLOW)

FPT_FDI_EXP.1

The only physical Shared-medium interface of the TOE is the Ethernet port directly controlled by the network controller.

The TOE controls and restricts the data/information flow from the Local User Interface (LUI), document scanner and document feeder to the network controller (which covers the information flow to and from the internal network). All data and/or commands received from these interfaces are processed and in most cases transformed by the copy controller before being submitted to the network controller. The network controller further processes the data before sending them to the internal network.

The TOE provides separation between the optional FAX processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, the Network Controller process and the FAX software process has no direct interface to communicate with each other without using the Copy Controller process as an intermediary. All internal command calls (API) and response messages for both the Network Controller process and the FAX software process are statically defined within the TOE. No user or system administrator is able to change their formats or functionalities.

The Fax software runs two independent processes, for sending and receiving job data through the fax card respectively. There is no internal communication between these two processes.

The same job data will never be active on both the fax interface and network interface at the same time. For network interface to fax interface (LanFax) jobs, the entire job must be received as an image and buffered in memory before it is sent out through the fax interface. Likewise, for fax interface to network interface (fax forwarding to email) jobs, the entire job must be received from the fax interface and buffered in controller memory before it is transformed by the copy controller process into an email attachment and sent out through the network interface.

7.1.3. Authentication (TSF_ AUT)

FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FMT_SMR.1, FTA_SSL.3

Under its evaluated configuration the TOE maintains two user roles, the "System Administrator" and "Standard User". A "System Administrator" has (or is given) access to all pathways, services and features including all management functions on the TOE. A "Standard User" is someone who has a unique ID maintained in the TOE and is not a System Administrator. In the context of this ST, "System Administrator" is equivalent to "U.ADMINISTRATOR" and "Standard User" is equivalent to "U.NORMAL".

All Users who are authorized to connect to the TOE can submit print or LanFax jobs.

A user must authenticate by entering a username and password prior to being granted access to the Local UI or the Web UI. While the user is typing the password, the TOE obscures[15] each character entered.

Upon successful authentication, users are granted access based on their role and predefined privileges. Only a system administrator is allowed full access to the TOE including all the system administration functions. Each common user's access is determined by which function (copy, scan, print, fax etc.) they have permission for.

If configured for local authentication the system requires the system administrator to enter a username and password for each user. The system will authenticate the user against an internal database.

By default, the Local UI will terminate any session that has been inactive for 1 minutes. By default, the Web UI will terminate any session that has been inactive for 60 minutes. The system administrator can configure both the Local UI and Web UI session timeouts to terminate an inactive session after some other period of time.

7.1.4. Network Identification (TSF_NET_ID)

FIA_UAU.7, FIA_UID.1, FIA_USB.1, FMT_SMR.1, FTA_SSL.3

As an alternative to TSF_AUT, the TOE allows user name and password for a user to be validated by a designated authentication server (a trusted remote IT entity). The user is not required to login to the network; account information entered at Local UI or Web UI of the TOE is authenticated at the server instead of the TOE. The remote authentication services[16] supported by the TOE are: CAC authentication, LDAP v4, Kerberos v5 (Solaris) and Kerberos v5 (Windows 2000/2003).

When a user authenticates using the CAC method a PIN number is used instead of a password. The PIN is authenticated by the CAC. If CAC is used for authentication, by default the Local UI will terminate a session that has been inactive for 6 minutes.

---

[15] The LUI obscures input with the asterisk character. The specific character used to obscure input at the WebUI is browser dependent.

[16] User account (authorization privilege) information can be maintained locally by the TOE or at the remote authentication server without impacting how a user session is presented or controlled; however, the use of remote authentication servers for this purpose is outside the scope of this evaluation.

The TOE maintains the username from a successful authentication during the context of the job, and this value is entered into the audit log as the *user name*.

7.1.5. Security Audit (TSF_FAU)

FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4, FMT_MTD.1 (MGMT1), FPT_STM.1

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to logged-in users, and each log entry contains a timestamp. The audit logs are only available to TOE administrators and can be downloaded via the web interface for viewing and analysis.

The audit log tracks user identification and authentication, system administrator actions, and failure of trusted channels. By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for transmission of data outside of the local environment, as required by such legislation as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc.

The Web UI presents the only access to the audit log; the audit log is not viewable from the Local UI. The system administrator must be logged in to download the audit log.

Application Note: For print and LanFax jobs not submitted from the web UI, the network username associated with the logged in user at the client workstation will be recorded in the audit log.

7.1.6. Cryptographic Operations (TSF_FCS)

FCS_COP.1

The TOE utilizes digital signature generation and verification (RSA), data encryption (TDES, AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) to support secure communication between the TOE and remote trusted products. Those packages meet the following standards: 3DES – FIPS 46-3 (cert #826 and cert # 1174); AES - FIPS 197 (cert #1131 and cert# 1821); SHA-1, SHA-256 – FIPS 180-3 (cert # 1599), HMAC - FIPS 198 (cert #644 and cert # 1076); RSA - FIPS 186-3 (cert # 914).

7.1.7. User Data Protection – Disk Encryption (TSF_FDP_UDE)

FCS_COP.1

The TOE utilizes data encryption (AES) to support encryption and decryption of designated portions of the hard disk where user files may be temporarily stored. The algorithm deployed meets the following standard: AES-CBC-256-FIPS-197 (CAVP Certificate No. 1131).

7.1.8. User Data Protection – IP Filtering (TSF_FDP_FILTER)

FDP_IFC.1 (FILTER), FDP_IFF.1 (FILTER), FMT_MTD.1 (FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is defined by the system administrator through specifying a series of rules to "accept," "deny," or "drop" packets. These rules include a listing of IP addresses that will be

allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

Note: The TOE cannot enforce the IP Filtering (TSF_FDP_FILTER) security function when it is configured for IPv6.

7.1.9. Network Security (TSF_NET_SEC)

FTP_ITC.1

The TOE supports various secure communication protocols as part of its security solution. These includes: SSL for Web UI; SSL for document transfers to the remote file depository; IPSec for communication over IPv4 and IPv6; and Kerberos or SSL for remote authentication.

7.1.10. Security Management (TSF_FMT)

FDP_ACC.1 (USER), FDP_ACC.1 (FUNC), FDP_ACF.1 (USER), FDP_ACF.1 (FUNC), FIA_ATD.1, FMT_SMF.1, FMT_MSA.1 (USER), FMT_MSA.1 (FUNC), FMT_MSA.3 (USER), FMT_MSA.3 (FUNC), FMT_MTD.1 (MGMT1), FMT_MTD.1 (MGMT2), FMT_MTD.1 (KEY), FTP_TST.1

Only authenticated system administrators can enable or disable the Image Overwrite function, change the system administrator password, and invoke an On Demand Image Overwrite operation.

While IIO can be disabled, doing so will remove the TOE from its evaluated configuration.

Additionally, only authenticated system administrators can assign authorization privileges[17] to users, create user IDs for local authentication, establish a recurrence schedule for On Demand Image Overwrite, enable/disable SSL support, enable/disable and configure IPSec, enable/disable and configure SNMPv3, create/install X.509 certificates, configure USB ports, enable/disable and configure fax to email forwarding, enable/disable and download the audit log, enable/disable and configure (rules) IP filtering, enable/disable disk encryption, enable/disable and configure use of Common Access Cards, configure inactive session timeout settings, verify the integrity of TOE software binary code, and enable/disable and configure 802.1x.

Only authenticated users with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the Web UI or the LUI.

All Users who are authorized to connect to the TOE can submit print or LanFax jobs.

All System Administrators are allowed full access to perform copy, print, scan or fax operations on the TOE.

Copy has to be performed at the local user interface. A user can only read physical copies of the documents (D.DOC +CPY Read). During job setup, a copy job (D.FUNC +CPY Delete, Modify) or image (D.DOC +CPY Read, Delete) can be read, modified or deleted. Once a job is

[17] User account (authorization privilege) information can be managed locally at the TOE or at a remote authentication server without impacting how a user session is presented or controlled; however, the use of remote authentication servers for this purpose is outside the scope of this evaluation.

committed, the job (D.FUNC +CPY Delete, Modify) can only be canceled (deleted) during its execution. Once completed, the job is removed.

Print jobs can be submitted remotely via printing protocols (e.g. lpr, port 9100) or from the WebUI using https. In which case, the owner should always assign a pass code on the job during its submission (i.e. a secure print job submission). In order to release printing of the document (D.DOC +PRT Read), the owner will need to be authenticated at the LUI and enter the correct pass code.

An authenticated job owner may also choose to submit and release print jobs at the Local UI from an USB storage device.

Once a print job is submitted to the TOE, there is no way for anyone to modify the job (D.FUNC +PRT Modify) or the document (D.DOC +PRT Delete). The authenticated owner may delete a print job (D.FUNC +PTR Delete) at the local user interface or through the Web UI (if the job is original submitted from the Web UI) before it is released.

A system administrator has the capability for deleting (D.FUNC +PRT Delete) any print job on the TOE through its authenticated Local UI or Web UI[18] session.

Once completed, a print job is removed.

Documents can only be scanned at the Local User Interface. During job setup, document image (D.DOC +SCN Read, Delete) may be read or deleted. Once the job is committed, the owner may send the image via email, transfer the image to a remote (SSL scan) repository, keep the image in their private mailbox or transfer the image to his/her personal USB storage device. (Scan to) Mailboxes are created and owned by individual users. Only the owner is allowed to locate and access the mailbox, and this access to mailboxes is further restricted with a pass code which the owner creates and owns. System Administrators have access to all the (scan) mailboxes. (Scan) Images saved in a mailbox (D.DOC +DSR and +SCN Read, Delete) may only be downloaded via the Web UI or deleted. A user with proper access may choose to delete the mailbox together with all images stored inside the mailbox.

Faxes can be submitted at the Local User Interface or remotely as LanFax (through printing protocol interfaces as for printing). During job setup, document image (D.DOC +FAXOUT Read, Delete) created may be read or deleted. Once a job (D.FUNC +FAXOUT Delete) is submitted, only a system administrator can delete the Job before it is fully completed, e.g. in the case of delayed send.

Access to the received Faxes (D.DOC +FAXIN Read, Delete) is restricted to the system administrators. All received faxes will be stored locally and assigned a (system administrator) predefined pass code. The SA can print or delete secure received faxes by entering the appropriate pass code. Once printed, the faxes are automatically deleted. Alternatively, the system administrator may also choose designate email addresses for receiving fax images. Once the fax job is forwarded as an attachment to an email, the job is automatically deleted.

Following recommendations from the user guidance document, an authenticated system administrator can perform various tests to verify the integrity of the TSF.

[18] At the Web UI, the System Administrator can only delete print jobs submitted from the Web UI.

During start up of the TOE after a reboot or power reset, an IIO is performed on U.DOC remaining inside the TOE's hard drive. Upon IIO completion, for a randomly picked contiguous block of disk space which is 10 % the size of the overall overwritten image, the resulting binary data pattern on the hard drive is compared against the expected results, and any mismatch would be reported. Also during initial start up, the version number of the software loaded is compared to the expected software version number; any corruption of this data will be reported.

During normal operation of the TOE, integrity of the IP filtering table can be verified through manual inspection from the Web UI, by the system administrator. The System Administrator can also verify the integrity of the TOE software image through the Web UI using a software verification feature.

8. GLOSSARY (NORMATIVE)

For the purposes of this document, the following terms and definitions apply. IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards, Seventh Edition,* should be referenced for terms not defined in this annex.

Access: Interaction between an entity and an object that results in the flow or modification of data.

Access Control: Security service that controls the use of hardware and software resources and the disclosure and modification of stored or communicated data.

Accountability: Property that allows activities in an IT system to be traced to the entity responsible for the activity.

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 TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Asset: An entity upon which the TOE Owner, User, or manager of the TOE places value.

Authentication: Security measure that verifies a claimed identity.

Authentication data: Information used to verify a claimed identity.

Authorization: Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized User: An authenticated User who may, in accordance with the TSP, perform an operation, This includes Users who are permitted to perform some operations but may be able to attempt or perform operations that are beyond those permissions.

Availability: (A) A condition in which Authorized Users have access to information, functionality and associated assets when requested. (B) Timely (according to a defined metric), reliable access to IT resources.

Channel: Mechanisms through which data can be transferred into and out of the TOE.

Confidentiality: (A) A condition in which information is accessible only to those authorized to have access. (B) A security policy pertaining to disclosure of data.

Enterprise: An operational context typically consisting of centrally-managed networks of IT products protected from direct Internet access by firewalls. Enterprise environments generally include medium to large businesses, certain governmental agencies, and organizations requiring managed telecommuting systems and remote offices

Evaluation Assurance Level: An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Interface: A non-hardcopy interface where either the input is being received from outside the TOE or the output is delivered to a destination outside the TOE.

Function: an entity in the TOE that performs processing, storage, or transmission of data that may be present in the TOE.

Hardcopy Device (HCD): A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones", and other similar products. See also: multifunction device.

Hardcopy Output Handler: Mechanisms for transferring User Document Data in hardcopy form out of the HCD.

Identity: A representation (e.g., a string) uniquely identifying an Authorized User, which can either be the full or abbreviated name of that User or a pseudonym.

Information assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT): The hardware, firmware and software used as part of a system to collect, create, communicate, compute, disseminate, process, store or control data or information.

Integrity: (A) A condition in which data has not been changed or destroyed in an unauthorized way. (B) A security policy pertaining to the corruption of data and security function mechanisms.

Job: A document processing task submitted to the hardcopy device. A single processing task may process one or more documents.

Multifunction Device (MFD) and **Multifunction Product (MFP)**: A hardcopy device that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

Nobody: A pseudo-role that cannot be assigned to any User.

Nonvolatile storage: Computer storage that is not cleared when the power is turned off.

Normal User: A User who is authorized to perform User Document Data processing functions of the TOE.

Object: A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation: A specific type of action performed by a subject on an object.

Operational Environment: The total environment in which a TOE operates, including the consideration of the value of assets and controls for operational accountability, physical security and personnel.

Operator Panel: A local human interface used to operate the HCD. It typically consists of a keypad, keyboard, or other controls, and a display device.

Organizational Security Policy (OSP): A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Original Document Handler: Mechanisms for transferring User Document Data in hardcopy form into the HCD.

Own or **Ownership**: May refer to a User Document or to User Function Data associated with processing a User Document. Depending upon the implementation of conforming TOE applications, the Owner of a User Function Data associated with a User Document may be different or may have different access control rules. These should be specified in a conforming Security Target.

Private-medium interface: Mechanism for exchanging data that (1) use wired or wireless electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous users; or, (2) use Operator Panel and displays that are part of the TOE.

Protected: A condition in which data has not been changed or destroyed in an unauthorized way.

Removable nonvolatile storage: nonvolatile storage that is part of an evaluated TOE but is designed to be removed from the TOE by authorized personnel. See also Nonvolatile storage.

Security attribute: A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP): A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Functional Requirement (SFR): A functional requirement which is taken from Part 2 of the Common Criteria and provide the mechanisms to enforce the security policy.

Security Target (ST): An implementation-dependent statement of security needs for a specific identified TOE.

SFR package: A named set of security functional requirements.

Shared-medium interface: Mechanism for transmitting or receiving data that uses wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users.

Subject: An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Telephone line: An electrical interface used to connect the TOE to the public switch telephone network for transmitting and receiving facsimiles.

Threat: Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

TSF Data: Data created by and for the TOE, that might affect the operation of the TOE.

TSF Confidential Data: Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.

TSF Protected Data: Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

TOE Owner: A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

TOE security functionality (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

User: An entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data: Data created by and for the User, that do not affect the operation of the TOE security functionality.

User Document Data: The asset that 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.

User Function Data: The asset that consists of the information about a user's document or job to be processed by the HCD.

9. ACRONYMS (INFORMATIVE)

For the purposes of this document, the following acronyms and definitions apply. IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards, Seventh Edition,* should be referenced for terms not defined in this annex.

Table 28: Acronyms

Acronym	Definition
A.	assumption (when used in hierarchical naming)
ADMIN.	administrator (when used in hierarchical naming)
ALT	alteration
CC	Common Criteria
C/IA	IEEE Computer Society Information Assurance
CONF.	confidential (when used in hierarchical naming)
CPY	copy
D.	data (when used in hierarchical naming)
DIS	disclosure
DOC.	document (when used in hierarchical naming)
DSR	document storage and retrieval
EAL	evaluation assurance level
F.	Function (when used in hierarchical naming)
FAX	facsimile
FUNC.	function (when used in hierarchical naming)
HCD	hardcopy device
IEEE	Institute of Electrical and Electronics Engineers
IOT	Image Output Terminal
IPP	Internet Printing Protocol
IT	information technology
LPR	Line Printer Remote
MFD	multifunctional device
MFP	multifunctional product / peripheral / printer
NVS	nonvolatile storage
O.	security objective (of the TOE) (when used in hierarchical naming)
OE.	security objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PP	protection profile
PROT.	protected (when used in hierarchical naming)
PRT	print
SCN	scan
SFP	security function policy
SFR	security functional requirement
SMI	shared-medium interface
ST	security target
Std	standard
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality

Acronym	Definition
TSP	TOE security policy
U.	user (when used in hierarchical naming)

10. BIBLIOGRAPHY (INFORMATIVE)

[B1] Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3 - Part 1: Introduction and General Model

[B2] Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3 - Evaluation Methodology

[B3] IEEE Std. 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition, New York, Institute of Electrical and Electronics Engineers, Inc.[19]

[19] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org)