Xerox WorkCentre 4250 / 4260 Multifunction Systems Security Target

Prepared by:

Xerox Corporation
1350 Jefferson Road
Rochester, New York 14623

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

Document Version: 1.0 (November 2010).

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 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC) v3.1, 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) 3 augmented with ALC_FLR.3.

ST Title:	Xerox WorkCentre 4250/4260 Multifunction Systems Security Target
ST Version:	1.0
Revision Number:	Revision 1.9
Publication Date:	November 17, 2010
Authors:	CSC Security Testing and Certification Laboratories, Xerox Corporation
TOE Identification:	Xerox WorkCentre 4250/4260 Multifunction Systems (see Section 1.4.1 for software version numbers)

ST Evaluator: CSC Australia CCTL

Keywords: Xerox, Multi Function Device, Image Overwrite, Mono, Hardcopy, Paper, Document, Printer, Scanner, Copier, Facsimile, Fax, Document Server, Document Storage and Retrieval, 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, Security Target

1.2 TOE Overview

1.2.1 Usage and Major Security Features

The TOE is a multi-function device (MFD) that provides copy and print services as well as the scan to e-mail, network scan and FAX options. A standard component of the TOE is the Image Overwrite Security package. This function forces any temporary image files created on the hard disk drive (HDD) during a copy (landscape/stapled type only), print, fax, network scan, or scan to e-mail job to be overwritten when those files are no longer needed, or "on demand" by the system administrator.

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

Table 1: Models and capabilities

(X – included in all configurations; o – product options ordered separately; n/a - not available)

	Print	Copy[1]	Network Scan	FAX[1]	Scan to e-mail	Print Speed
WorkCentre 4250	n/a	X	n/a	n/a	n/a	Up to 45ppm
WorkCentre 4250s	X	X	X	o	X	Up to 45ppm
WorkCentre 4250x	X	X	X	X	X	Up to 45ppm
WorkCentre 4250xf	X	X	X	X	X	Up to 45ppm
WorkCentre 4260s	X	X	X	o	X	Up to 55ppm
WorkCentre 4260x	X	X	X	X	X	Up to 55ppm
WorkCentre 4260xf	X	X	X	X	X	Up to 55ppm

An optional Finisher which is not part of the TOE provides "after print" services such as document collation and stapling.

A MFD stores temporary image data created during a copy (landscape/stapled type only), print, fax, network scan, or scan to e-mail job on an internal hard disk drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDDs used for spooling temporary files are encrypted. The encryption key is created dynamically on each power-up.

NOTE: Print, fax, network scan and scan to e-mail jobs are written directly to the HDD when the job enters the system. Copy jobs are buffered in volatile memory with one exception: only copy jobs of type "landscape/stapled" are written to the disk. Any data that gets written to the disk will be overwritten at the completion of the job. "Copy/Print, Store and Reprint" (CPSR) jobs are written to the hard drive so that they may be reprinted at a later time; therefore, they will be overwritten when a full on-demand image overwrite is performed.

The TOE provides an Image Overwrite function to enhance the security of the MFD. The Image Overwrite function overwrites temporary document image data as described in DoD Standard 5200.28-M[1] at the completion of each copy (landscape/stapled type only), print, fax, network scan, or scan to e-mail job, once the MFD is turned back on after a power failure or *on demand* of the MFD system administrator.

User image files associated with the "Copy/Print, Store and Reprint" feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job using the 5200.28-M algorithm. The stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite. 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 all files that have been stored at the request of a user via Copy/Print, Store and Reprint jobs.

All models of the TOE support network security. The system administrator can enable and configure the network security support. The network security support is based on SSL. When SSL support is enabled on the device, the following network security features can be enabled/configured: HTTPS support (for both the device's Web UI and network scan data transfer); system administrator download of the device's audit log; IPSec support for IPP, lpr and port 9100 print jobs; secure network device management through SNMPv3, and specification of IP filtering rules. Scan-to-email and FAX data are not protected from sniffing by the IPSec or SSL support. The transmission of LanFax data over the Ethernet connection is protected by IPSec, but the transmission over the PSTN is not. Note that IPSec and SNMPv3 can only be activated if SSL has been enabled and an SSL-based certificate (either "self-

[1] DoD 5200.28-M, Section VII, Part 2: "…all storage locations will be overwritten a minimum of three times, once with the binary digit "1," once with the binary digit "0," and once with a single numeric, alphabetic, or special character. Such alpha-numeric or other unclassified data shall be left on the device. The current used in overwriting must be equal to that used in recording the information, but of a strength that will not damage or impair the equipment."

signed" or generated by an external Certificate Authority) has been loaded into the TOE via the Web UI. Once this has occurred, SSL could be disabled.

1.3 TOE Type

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

1.3.1 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 features are only useful in environments where the TOE is connected to a network. TSF_NET_AUT is only available when one of the following remote authentication services is present on the network that the TOE is connected to: LDAP, Kerberos, or SMB.

1.4 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.

1.4.1 Physical Scope of the TOE

The TOE is a Multi-Function Device (Xerox WorkCentre models 4250 and 4260) that provides copying, printing, faxing, scan to e-mail and network scanning. All models of the TOE include Administrator and User guidance. The WC4250 operates at a maximum of 45 pages per minute (ppm) and the WC4260 operates at a maximum of 55ppm. The WC4260 does not have a copier-only configuration. The differences between the various models is the package of optional features selected by the consumer (see **Table 1**).

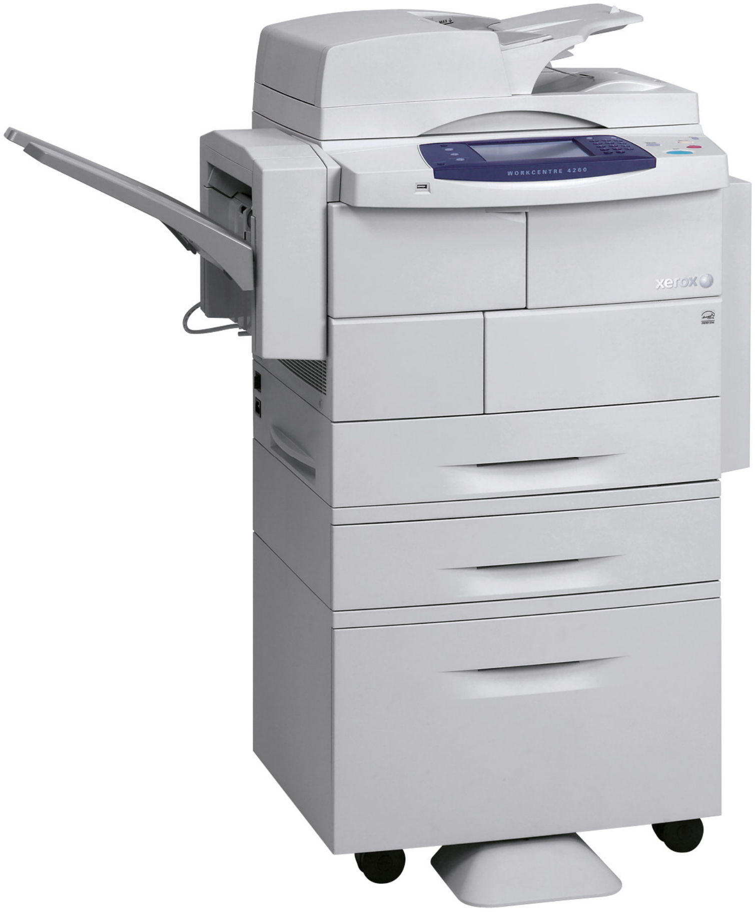

Figure 1: Xerox WorkCentre 4250 / 4260

The hardware included in the TOE is shown in **Figure 1: Xerox WorkCentre 4250 / 4260**. While this figure does show the three optional paper trays (bottom) and optional finisher (left side of the photograph), the optional FAX card is an internal component that is not visible.[2]

The various software and firmware ("Software") that comprise the TOE are listed in Table 2: Evaluated Software/Firmware version. A system administrator can ensure that they have a TOE by printing a configuration

[2] 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.

sheet and comparing the version numbers reported on the sheet to the table below.

The **System software** number is a designator that signifies the aggregation of the following set of software components. The **UI software** controls the User Interface. **IOT software** controls the marking engine that prints to paper. **Document Feeder software** controls the input tray. **Finisher software** controls the optional Finisher attachment. **Tray Firmware** controls the operation of optional paper feeder trays. The **Main Controller software** resides on the Main Controller and controls copy, fax, print, scan, scan to email, and security functions.

Table 2: Evaluated Software/Firmware version

Software/Firmware Item	Optional?	WorkCentre 4250	WorkCentre 4260
System Software	**No**	**15.003.32.000**	**30.103.32.000**
Main Controller	**No**	**2.50.03.32**	**2.50.03.32**
IOT Software	**No**	**0.01.17**	**0.40.59**
UI	**No**	**0.045.15.027**	**0.040.15.176**
Network Controller	**No**	**4.01.23**	**4.01.67**
Document Feeder Software	**No**	**1.01**	**1.01**
Finisher Software	**Yes**	**4.04.09**	**4.04.09**
Tray Firmware	**Yes**	**1.01.04**	**1.01.04**

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 guidance by comparing the software version number, displayed when the CD is initially run, to the version numbers listed in the table below.

Table 3: System User and Administrator Guidance

Title	Version
User Documentation (CD1)	538N00084 revA
Drivers (CD2)	538N00085 revA
Drivers (CD3)	538N00086 revA
Scanning Software (CD4)	538N00087 revA
System Administrator Guide (CD5)	538N00088 revA

The TOE's physical interfaces include a power port, Ethernet port, two Type A USB ports, one Type B USB port, FAX port (if the optional FAX card is installed), finisher connection port, SIM slot, Local User Interface (LUI) with keypad, a document scanner, a document feeder and a document output.

1.4.2 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: Evaluated Software/Firmware version). The TOE logical boundary is composed of the security functions provided by the product.

The following security functions are provided by the TOE:

- Image Overwrite (TSF_IOW)
- Information Flow (TSF_FLOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSEC)
- Network Management Security (TSF_NET_MGMT)
- Security Management (TSF_FMT)
- User Data Protection –AES (TSF_EXP_UDE)

1.4.3 Image Overwrite (TSF_IOW)

The TOE has an “Image Overwrite” function that overwrites files created during copy (landscape/stapled type only), print, fax, network scan or scan to e-mail jobs. This overwrite process is implemented in accordance with DoD 5200.28-M and will be activated at the completion of each copy (landscape/stapled type only), print, fax, network scan, or scan to e-mail job, once the MFD is turned back on after a power failure or *on demand* of the MFD system administrator. Copy/Print, Store and Reprint jobs are written to the hard drive so that they may be reprinted at a later time; therefore, they will be overwritten when a full on-demand image overwrite is performed.

User image files associated with the Copy/Print, Store and Reprint feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job using the 5200.28-M algorithm. The stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite.

1.4.4 Information Flow (TSF_FLOW)

The TOE controls and restricts the information flow between the PSTN port of the optional FAX board (if installed) and the network port of the main controller. Data and/or commands cannot be sent to the internal network via the PSTN. 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.

1.4.5 System Authentication (TSF_SYS_AUT)

The TOE requires a system administrator to authenticate before granting access to system administration functions. The system administrator has to enter a PIN at either the Web User Interface or the Local User Interface. The PIN will be obscured with asterisks as it is being entered. Identification of the system administrator at the Local User Interface is implicit -- the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window.

1.4.6 Network Authentication (TSF_NET_AUT)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server (a trusted remote IT entity). The user is not required to login to the network; the account is authenticated by the server as a valid user. The remote authentication services supported by the TOE are: LDAP, Kerberos (Solaris), Kerberos (Windows 2000/2003), and SMB (Windows NT.4x/2000/2003).

1.4.7 Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs 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™.

1.4.8 Cryptographic Operations (TSF_FCS)

The TOE utilizes data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-186, SSLv3.

NOTE: the strength of the cryptographic algorithms supported by the TOE is not part of the evaluation.

1.4.9 User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing (SSLSec SFP). SSL must be enabled before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option.

1.4.10 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” packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE.

1.4.11 User Data Protection – IPSec (TSF_FDP_IPSec)

The TOE implements the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE. Printing clients initiate the establishment of a security association with the MFD. The MFD establishes a security association with the printing client using IPSec “tunnel mode.” Thereafter, all IP-based traffic to and from this destination will pass through the IPSec tunnel until either end powers down, or resets, after which the tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client. IPSec does not protect scan-to-email or FAX data. The transmission of LanFax data over the Ethernet connection is protected by IPSec, but the transmission over the PSTN is not. The TOE implements IPSec for both IPv4 and IPv6; however, IPSec is not available for,AppleTalk or IPX.

Note: The TOE cannot enforce the IPSec (TSF_FDP_IPSec) security function when it is configured for AppleTalk or IPX networks.

1.4.12 Network Management Security (TSF_NET_MGMT)

The TOE supports SNMPv3 as part of its security solution through the SNMPSec SFP. The SNMPv3 protocol is used to authenticate each SNMP message, as well as, provide encryption of the data as described in RFC 3414.

As implemented, both an authentication and privacy (encryption) password must be set up both at the device and at the manager. Both passwords must be a minimum of 8 characters. SNMP uses SHA-1 for authentication.

1.4.13 Security Management (TSF_FMT)

Only authenticated system administrators can perform the following operations:

- Enable or disable Immediate Image Overwrite;
- Enable or disable On-Demand Image Overwrite;
- Change the system administrator PIN;
- Manually invoke "On Demand" Image Overwrite.
- Enable or disable SSL support;
- Create and install X.509 certificates;
- Enable, disable and download the audit log;
- Enable, disable and configure (rules) IP filtering;
- Enable, disable and configure IPSec;
- Enable, disable and configure IPv6;
- Enable, disable and configure SNMPv3;
- Configure network authentication.

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

1.4.14 User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation to support encryption and decryption of designated portions of the hard disk where user files may be stored. Those packages include provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-192-FIPS-197.

1.4.15 Evaluated Configuration

In its evaluated configuration, IIO and ODIO are enabled on the TOE. The FAX option, if purchased by the consumer, is installed and enabled. While the TOE will be evaluated with SSL enabled, this security feature should be configured and enabled or disabled in accordance with the consumer's established security policies. All other configuration parameter values are optional.

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 1, CCMB-2006-09-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2007-09-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

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

2.2 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profile

2.3 Package Claims

This Security Target claims conformance to the EAL3 package augmented with ALC_FLR.3.

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 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/system administrator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

Table 4: Environmental Assumptions

Assumption	Description
A.INSTALL	The TOE has been delivered and installed by Xerox-authorized representatives using Xerox delivery and installation guidance. The TOE has been configured by the system administrator in accordance with the administrator and user guidance delivered with the TOE as well as the security guidance found at http://www.xerox.com/security. As a part of this installation process, the system administrator has changed the PIN from its default value. The PIN chosen by the administrator consists of at least 8 characters and will be changed at least every 40 days. IIO and ODIO are enabled.
A.ACCESS	The TOE has been installed in a standard office environment. Because the TOE is under observation by office personnel, unauthorized physical modifications to the TOE and unauthorized attempts to connect to the TOE via its physical interfaces are not possible.
A.MANAGE	One or more system administrators are assigned to manage the TOE. Procedures exist for granting a system administrator access to the system administrator PIN for the TOE.

Assumption	Description
A.NO_EVIL_ADM	The system administrator(s) are not careless, willfully negligent or hostile, and will follow the instructions provided in the administrator and user guidance delivered with the TOE as well as the security guidance found at http://www.xerox.com/security. The system administrator will not remove the TOE from its evaluated configuration and will especially not disable TSF_IOW.
A.NETWORK	The network that the TOE is connected to will be monitored for unapproved activities and/or attempts to attack network resources (including the TOE).
A.SANE_NETWORK	All network components connected to the network to which the TOE is connected pass data correctly without modification.
A.SAME_CONTROL	All of the systems that communicate with the TOE are under the same management and physical control as the TOE and are covered by the same management and security policy as the TOE.
A.EXT_RFC_COMPLIANT	All of the remote trusted IT products that communicate with the TOE implement the external half of the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (i.e., SSL) and work as advertised.
A.CHANGE_SA_PIN	System administrators PIN is changed according to the following: 8-character PIN every 40 days 9-character PIN every year
A.PROCEDURE	Procedures exist for granting system administrator(s) access to the TSF.

3.2 Threats

3.2.1 Threats Addressed by the TOE

Table 5 identifies the threats to the TOE. The various attackers of the TOE are considered to be either authorized or unauthorized users of the TOE with public knowledge of how the TOE operates. These users do not have any specialized knowledge or equipment. The authorized users have physical access to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 5: Threats to the TOE

Threat	Description

Threat	Description
T.RECOVER	A malicious user may attempt to recover temporary document image data using commercially available tools to read its contents. This may occur because the attacker gets physical access to the hard disk drive (e.g. as part the life-cycle of the MFD (e.g. decommission)), or the temporary document image data can be read/recovered over the network (e.g. as the result of a purposeful or inadvertent power failure before the data could be erased.)
T.INFAX	During times when the FAX is not in use, a malicious user may attempt to access the internal network by connecting to the FAX card via PSTN and using publicly available T.30 FAX transmission protocol commands for the purpose of intercepting or modifying sensitive information or data that may reside on resources connected to the network. This threat only exists if the FAX board is installed and connected to the PSTN.
T.OUTFAX	During times when the FAX is not in use, a malicious user may attempt to connect to the TOE over the network and make an outgoing connection using the FAX card, either as a method of attacking other entities or for the purpose of sending sensitive information or data to other entities.[3] This threat only exists if the FAX board is installed and connected to the PSTN.
T.USER	A user, at any time, may attempt to reconfigure the TOE, for the purpose of disabling security functions or intercepting sensitive information or data, either by attempting to access the management functions directly or by logging in as the system administrator.
T.COMM_SEC	An attacker may break into a communications link between the TOE and a remote trusted IT product in order to intercept, and/or modify, information passed to/from/between the TOE and remote trusted IT product.
T.TOE_SEC	An attacker may use the network as a conduit to attempt to break into the TOE WebUI by using vulnerabilities or carefully crafted packets.

3.2.2 Threats Addressed by the IT Environment

Table 5 identifies the threats to the IT Environment. The various attackers of the IT Environment are considered to be either authorized or unauthorized users of the IT Environment with public knowledge of how the IT Environment operates. These users do not

[3] *Application Note: The sending of company confidential information to external entities by Fax is not considered a threat to the TOE.*

have any specialized knowledge or equipment. The authorized users have physical access to the IT Environment. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 6: Threats Addressed by the IT Environment

Threat	Description
TE.COMM_SEC	An attacker may break into a communications link between the TOE and a remote trusted IT product in order to intercept, and/or modify, information passed to/from/between the TOE and remote trusted IT product.

3.3 Organizational Security Policies

Table 7 below enumerates the organizational security policies the TOE must comply with:

Table 7: Organizational Security Policy(s)

Policy	Description
P.COMMS_SEC	TOE supported network security mechanisms (i.e., IP filtering) shall be employed per, and in accordance with, local site security policy.
P.HIPAA_OPT	(Appropriate to organizations under HIPAA oversight) All audit log entries (scan) will be reviewed periodically (the period being local site specific and to be determined by the local audit cyclic period) and in accordance with 45 CFR Subtitle A, Subchapter C, Part 164.530(c),(e),(f) which covers safeguards of information (c), sanctions for those who improperly disclose (e), and mitigation for improper disclosures (f). [4]
P.SSL_ENABLED	Secure Socket layer network security mechanisms shall be supported by the TOE and employed as dictated by local site policy.

[4] "HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business. HIPAA seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.." (Definition from TechTarget)

See http://www.hhs.gov/ocr/hipaa/ for more information about HIPAA.

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 identifies and describes the security objectives of the TOE.
The TOE accomplishes the security objectives defined in Table 8.

Table 8: Security Objectives for the TOE

Objectives	Description
O.AUDITS	The TOE must record, protect, and provide to system administrators audit records relative to data scan transmissions through the TOE that (may) have HIPAA-privileged information.
O.RECOVER	Temporary document image data from a copy (landscape/stapled type only), print, fax, network scan or scan to e-mail job must be overwritten on the hard disk drive in accordance with DoD 5200.28-M immediately after that job is completed or once the TOE is turned back on after a power failure. Temporary document image data from these jobs must also be overwritten at the command ("on demand") of the system administrator.
O.FAXLINE	The TOE will not allow access to the internal network from the telephone line via the TOE's FAX modem (if installed). Likewise, the TOE will not allow accessing the PSTN port of the TOE's FAX modem (if installed) from the internal network.
O.MANAGE	The TOE will provide the functions and facilities necessary to support system administrators responsible for the management of the TOE. The TOE must require that system administrator(s) authenticate with a PIN before allowing access to management functions. The PIN must be obscured as it is entered by the system administrator. The Local UI will be locked until power is cycled or until 3 minutes

Objectives	Description
	have passed once 3 invalid login attempts have been detected. The WebUI will send an error code after every invalid authentication attempt.
O.CONTROL_ACCESS	The TOE will provide the system administrator with the ability to determine network access/information flow to and/or from the TOE and to and/or from trusted remote IT products.
O.PROTECT_COM	The TOE must protect user data from disclosure, or modification, by establishing a trusted channel between the TOE and another trusted IT product over which the user data is transported.

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 9: Security Objectives for the IT Environment

Objectives	Description
OE.NETWORK	The network that the TOE is connected to will be monitored for unapproved activities and/or attempts to attack network resources (including the TOE). This includes a high number of logon tries to the web interface of the TOE.

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 10: Security Objectives for the Non-IT Environment

Objectives	Description

Objectives	Description
OE.INSTALL	System administrator oversees installation, configuration and operation of the TOE by Xerox-authorized representatives in accordance with the Xerox delivery and installation guidance. The TOE must be configured by the system administrator in accordance with the system administration and user guidance as well as with the security guidance found at http://www.xerox.com/security. As part of the installation process, the system administrator has to change the PIN from its default value to a value with at least 8 characters. The system administrator has to change the PIN at least every 40 days. The system administrator ensures that the TOE will be configured according to the configuration under evaluation and will not remove the TOE from its evaluated configuration. Especially Image Overwrite Security accessory is installed and enabled and IIO and ODIO are enabled.
OE.NETWORK_I&A	The TOE environment shall provide, per site specific policy, the correct and accurately functioning Identification and Authentication mechanism(s) that are compatible with, and for external use by, the TOE and which are under the same control as the TOE.
OE.ACCESS	The TOE will be located in an office environment where it will be monitored by the office personnel for unauthorized physical connections, manipulation or interference.
OE.ADMIN	At least one responsible and trustworthy individual (system administrator) will be assigned, according to onsite procedures for granting access to the PIN, to manage the TOE. The individual(s) have to follow the instructions provided in the administrator and user guidance as well as the security guidance found at http://www.xerox.com/security
OE.PROTECT_COM	The TOE environment must protect user data from disclosure, or modification, by establishing a trusted channel between itself and the TOE over which the data is transported prior to data transmission.

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 11: Completeness of Security Objectives

	OBJECTIVES											
Threats, Assumptions, OSPs	**O.AUDITS**	**O.RECOVER**	**O.FAXLINE**	**O.MANAGE**	**O.CONTROL_ACCESS**	**O.PROTECT_COM**	**OE.NETWORK**	**OE.INSTALL**	**OE.NETWORK_I&A**	**OE.ACCESS**	**OE.ADMIN**	**OE.PROTECT_COM**
T.RECOVER		X										
T.INFAX			X									
T.OUTFAX			X									
T.USER				X			X					
T.COMM_SEC						X						
T.TOE_SEC					X							
TE.COMM_SEC												X
P.COMM_SEC						X						X
P.HIPAA_OPT	X											
P.SSL_ENABLED						X						X
A.INTALL								X			X	
A.ACCESS										X		
A.MANAGE											X	
A.NO_EVIL_ADMIN								X			X	
A.NETWORK							X					
A.SANE_NETWORK							X					
A.SAME_CONTROL									X		X	
A.EXT_RFC_COMPLIANT												X
A.CHANGE_SA_PIN											X	
A.PROCEDURE											X	

Table 12: Sufficiency of Security Objectives

Threats, Assumptions, and OSPs	Objective	Rationale

Threats, Assumptions, and OSPs	Objective	Rationale
T.RECOVER	O.RECOVER	O.RECOVER helps to mitigate the threat T.RECOVER to an acceptable level by minimizing the amount of time that temporary document image data is on the hard disk drive. O.RECOVER requires that the residual data will be overwritten as described in DoD 5200.28-M immediately after the job is finished or once the TOE is turned back on after a power failure. Additionally, O.RECOVER requires that the TOE perform the overwrite security function at any time that the system administrator chooses to ensure that all latent data has been removed.
T.INFAX T.OUTFAX	O.FAXLINE	O.FAXLINE counters the threat T.INFAX because a connection from the PSTN port of the FAX board (if installed) to the internal network is not allowed. O.FAXLINE counters the threat T.OUTFAX because the users of the internal network are not allowed to access the PSTN port of the FAX board (if installed). So, it is not possible to establish an interconnection between PSTN and the internal network by using the TOE.
T.USER	O.MANAGE OE.NETWORK	O.MANAGE counters the threat T.USER by ensuring that the users who have not authenticated as the system administrator cannot access the management functions and cannot make configuration or operational changes to the TOE that would remove it from the evaluated configuration or allow them to access job data. O.MANAGE also protects against brute-force attacks against the PIN at the local user interface. OE.NETWORK ensures that brute-force attacks against the PIN are also not possible at the web interface.
T.TOE_SEC	O.CONTROL_ACCESS	O.CONTROL_ACCESS helps mitigate the threat T.TOE_SEC by ensuring that the administrator has the ability to control network access and information flow to the WebUI by implementing IP Filter in order to determine which network resources are allowed to connect to the WebUI which will limit an attacker's access to the TOE.
T.COMM_SEC	O.PROTECT_COM	O.PROTECT_COM helps mitigate the threat T.COMM_SEC by ensuring that a fully-compliant

Threats, Assumptions, and OSPs	Objective	Rationale
		trusted channel between the TOE and another remote trusted IT product exists to protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
TE.COMM_SEC	OE.PROTECT_COM	OE.PROTECT_COM helps mitigate the threat TE.COMM_SEC by ensuring that a trusted communication channel between the TOE and remote trusted IT products is established to protect user data from disclosure or modification.
A.INSTALL	OE.INSTALL OE.ADMIN	OE.INSTALL covers A.INSTALL because the TOE will be delivered and installed by Xerox representatives according to all respective guidance documents. The TOE will be configured by the system administrator in accordance with the admin guidance of the TOE and the security guidance provided at the Xerox web site. This especially includes that the TOE is in the configuration under evaluation and that the Image Overwrite Security is installed and enabled. Furthermore, the default PIN was changed to a (at least) 8-characterPIN and the PIN will be changed at least every 40 days. OE.ADMIN covers A.INSTALL by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE.
A.ACCESS	OE.ACCESS	OE.ACCESS covers A.ACCESS because the TOE will be installed in standard office environment and the office personnel will monitor the TOE to prevent unauthorized physical access to the HDD and the TOEs interfaces.
A.MANAGE	OE.ADMIN	OE.ADMIN covers A.MANAGE by requiring at least one trustworthy and responsible person to oversee the installation and operation of the TOE. This person(s) will be assigned according to onsite procedures and will follow all TOE administrator guidance. “Assignment” means here the person(s) get knowledge about the PIN.
A.NO_EVIL_ADM	OE.INSTALL OE.ADMIN	OE.ADMIN covers parts of A.NO_EVIL_ADM because “*responsible and trustworthy individual*” are “*not careless, willfully negligent or hostile*”. Furthermore, the individuals have to follow the instructions

Threats, Assumptions, and OSPs	Objective	Rationale
		provided in the guidance documents. OE.INSTALL covers the remaining part of A.NO_EVIL_ADM because the objective ensures that the system administrator configures the TOE according to the configuration under evaluation and will not remove the TOE from its evaluated configuration (especially that the Image Overwrite Security accessory is installed and enabled).
A.NETWORK	OE.NETWORK	OE.NETWORK covers A.NETWORK by requiring a mechanism to detect network-based attacks against the TOE.
A.SAME_CONTROL	OE_NETWORK_I&A OE.ADMIN	OE.NETWORK_I&A supports the assumption A.SAME_CONTROL by ensuring the presence within the environment of a fully-functioning I&A mechanism to limit the ability of an attacker to intercept communications between the TOE and a remote trusted IT product. OE.ADMIN supports the assumption A.SAME_CONTROL by ensuring that such remote products are under the same management and subject to the same security policy as the TOE by assigning a competent administrator.
A.EXT_RFC_COMPLIANT	OE.PROTECT_COM	OE.PROTECT_COM ensures a trusted channel between the TOE and another remote trusted IT product exists to protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
A.CHANGE_SA_PIN	OE.ADMIN	OE.ADMIN covers A.CHANGE_SA_PIN because "*responsible and trustworthy individuals*" are "*not careless, willfully negligent or hostile*". Furthermore, the individuals have to follow the instructions provided in the guidance documents, including those that prescribe guidance for composition of the TOE SA PIN.
A.PROCEDURE	OE.ADMIN	OE.ADMIN covers A.PROCEDURE by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE.
A.SANE_NETWORK	OE.NETWORK	OE.NETWORK covers A.SANE_NETWORK by providing for monitoring of the environment such that data or protocol modification will be detected.
P.HIPAA_OPT	O.AUDITS	O.AUDITS helps satisfy OSP P.HIPAA_OPT by ensuring that log entries are provided by the TOE for

Threats, Assumptions, and OSPs	Objective	Rationale
		periodic review by system administrators, in order to ensure that safeguards for information mandated by applicable laws and regulations remain in place, and that audit logs available to mitigate the risk of improper disclosure and to support application of sanctions following improper disclosure.
P.COMM_SEC P.SSL_ENABLED A.EXT_RFC_COMPLIANT	O.PROTECT_COM	O. PROTECT_COM helps meet OSPs P.COMMS_SEC and P.SSL_ENABLED by ensuring that fully-compliant (A.EXT_RFC_COMPLIANT) trusted channel between the TOE and another remote trusted IT product exists to protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
P.COMMS_SEC P.SSL_ENABLED	OE.PROTECT_COM	OE.PROTECT_COM meet the OSPs P.COMMS_SEC AND P.SSL_ENABLED by ensuring that a trusted communication channel between the TOE and remote trusted IT products is established to protect user data from disclosure or modification.

5 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.

5.1 Security Policies

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

Note: The TOE cannot enforce the IP Filtering (TSP_FILTER), and IPSec (TSP_IPSEC) security policies when it is configured for AppleTalk or IPX networks.

5.1.1 User Data Protection Policy (TSP_IOW)

The image information of the different types of jobs the MFD can handle is considered as confidential user information. Therefore, the TOE must protect this information according to the following rules:

- Temporary document image data from a copy (landscape/stapled type only), print, workflow scan, fax, LanFax or scan-to-email job must be overwritten on the hard disk drives in accordance with DoD 5200.28-M immediately after that job is completed.
- All temporary document image data of abnormally terminated jobs on the HDDs must be overwritten in accordance with DoD 5200.28-M once the MFD is turned back on after a power failure.
- The space on the hard disk drives reserved for temporary document image data must be overwritten in accordance with DoD 5200.28-M, if the system administrator has invoked the On Demand Image Overwrite function.

- The space on the hard disk drives reserved for the Copy/Print, Store and Reprint image data must be overwritten in accordance with DoD 5200.28-M, if the system administrator has invoked the Full On Demand Image Overwrite function.

5.1.2 Information Flow Control Policy (TSP_FLOW)

The security function "Information Flow" (TSF_FLOW) (see section 6.1.2) restricts the information flow between the PSTN port of the optional FAX board (if installed) and the internal network by implementing a store-and-forward principle.

The following policy defines the rules according to which TSF_FLOW shall restrict the information flow, if the FAX board is installed:

- RECEIVING FAX: The FAX board must have terminated the PSTN connection before informing the copy controller about the fax currently received.
- SENDING FAX: The copy controller must have finished the copy operation of the fax image to the shared memory area of the FAX board before informing the FAX board to send the fax.

If the FAX board is not installed, an information flow is not possible and needs not to be restricted. However, it is not required that the copy controller works in this situation in a different way.

5.1.3 SSLSec SFP (TSP_SSL)

The security function "User Data Protection -- SSL" (TSF_FDP_SSL) requires that SSL is enabled so that Web-based network traffic to and from the TOE will be encrypted using SSL This policy will be enforced on:

- SUBJECTS: Web clients.
- INFORMATION: All web-based traffic to and from that destination.
- OPERATIONS: HTTP commands.

5.1.4 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 TCP or UDP-based traffic to and from that destination.
- OPERATIONS: Pass network traffic.

5.1.5 IPSec SFP (TSP_IPSEC)

The security function "User Data Protection -- IPSec" (TSF_FDP_IPSec) requires that network traffic to and from the TOE will be encrypted when the printing client initiates IPSec encryption. This policy will be enforced on:

- SUBJECTS: Printing clients.
- INFORMATION: All IP-based traffic to and from that destination.
- OPERATIONS: Print jobs.

5.1.6 SNMPSec SFP (TSP_SNMP)

The security function "Network Management Security" (TSF_NET_MGMT) requires that the TOE applies SNMPv3 so that network traffic to and from the TOE will be encrypted in accordance with SNMPv3. This policy will be enforced on:

- SUBJECTS: Remote SNMPv3 hosts.
- INFORMATION: All SNMPv3 traffic to and from that destination.
- OPERATIONS: SNMPv3 commands and messages.

5.1.7 PrivUserAccess SFP (TSP_FMT)

The security function "Security Management" (TSF_FMT) restricts management of TOE security functions to the authorized system administrator.

5.2 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 <u>*underlined and italic text*</u>.
- 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. "(SSL)"). The resulting component ID would be "FDP_IFC.1 (SSL)".
- Where an iteration is identified in rationale discussion as "all", the statement applies to all iterations of the requirement (e.g. "FCS_CKM.1 (all)")

5.3 Security Functional Requirements

The TOE satisfies the SFRs delineated in Table 13. The rest of this section contains a description of each component and any related dependencies.

Table 13: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Access control functions
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions
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_STM.1	Reliable time stamp
FPT_TST.1	TSF Testing
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

5.3.1 Class FAU: Security audit

5.3.2 FAU_GEN.1 Audit data generation

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
- [The events specified in Table 14 below].

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, [the events specified in Table 14 below].

Table 14: Audit Data Requirements

<table>
<tr><td colspan="3">The audit log will have the following fixed size entries:<ul><li>Entry number (an integer value from 1 to the number of entries in the audit log)</li><li>Event Date (mm/dd/yy)</li><li>Event Time (hh:mm:ss)</li><li>Event ID (a unique integer value – see table entries below)</li><li>Event Description (a brief description of an entry that should match the unique Entry ID value – see table entries below)</li><li>Entry Data (This value is any additional data that is logged for an audit log entry – see table entries below)</li></ul></td></tr>
<tr><th>Event ID</th><th>Event Description</th><th>Entry Data Contents</th></tr>
</table>

1	System startup	Device Name, Device Serial Number
2	System shutdown	Device Name, Device Serial Number
5	Print Job	Job name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID
6	Network Scan Job	Job name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID, total-number-net-destination, net-destination
7	Server Fax Job	Job name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID, Total-fax-recipient-phone-numbers, fax-recipient-phone-numbers, net-destination.
9	Email Job	Job name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID, total-number-of-smtp-recipients, smtp-recipients
10	Audit Log Disabled	Device name; Device serial number
11	Audit Log Enabled	Device name; Device serial number
12	Copy Job	Job Name, User Name, Completion Status, IIO status: 'Not-Supported', Accounting User ID, Accounting Account ID
13	Embedded Fax Job	Job Name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID, Total-fax-recipient-phone-numbers, fax-recipient-phone-numbers
14	Lan Fax Job	Job Name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID, Total-fax-recipient-phone-numbers, fax-recipient-phone-numbers

16	ODIO Standard Started	Device name; Device serial number
17	ODIO Standard Complete	Device name; Device serial number, Overwrite Status
18	ODIO Full Started	Device name; Device serial number
19	ODIO Full Complete	Device name; Device serial number, Overwrite Status
21	Delete File/Directory (CPSR)	Job name or Dir name, User Name, Completion Status, IIO status, Accounting User ID, Accounting Account ID
22	USB Thumb Drive	Job name or Dir name, User Name, Completion Status, IIO status: 'Not-Supported', Accounting User ID, Accounting Account ID
23	CPSR Store	Job name or Dir name, User Name, Completion Status, IIO status: 'Not-Supported', Accounting User ID, Accounting Account ID
24	CPSR Print	Job name or Dir name, User Name, Completion Status, IIO status: 'Not-Supported', Accounting User ID, Accounting Account ID

Application note: The data line of each field size entry might exceed the assigned size and will result in truncating the data in an entry.

5.3.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1:	The TSF shall provide [system administrator(s)] with the capability to read [all information] from the audit records.
FAU_SAR.1.2:	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.4 FAU_SAR.2Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

5.3.5 FAU_STG.1Protected 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.

5.3.6 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.

5.3.7 Class FCO: Communication

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

5.3.8 Class FCS: Cryptographic support

5.3.8.1FCS_CKM.1 (SSL 1) Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [as defined in the SSL v3 standard] and specified cryptographic key sizes [56-bit (DES), 128-bit (RC4), 168-bit (3DES) or smaller key sizes required for SSLv3 non-capable clients] that meet the following: [generation and exchange of session keys a defined in the SSL v3 standard with the cipher suites defined in FCS_COP.1 (SSL 2)].

Application note: *The SSLv3 standard defines the generation of symmetric keys in Section 6.2. The evaluation does not cover the assessment of the strength of the keys generated, ONLY that the keys are generated in accordance with the requirements specified in the standard.*

5.3.9 FCS_CKM.1 (SSL 2) Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA key pair generation] and specified cryptographic key sizes [1024 bits or smaller key sizes required for SSLv3 non-capable clients] that meet the following: [not specified].

Application note: *The SSL v3 standard does not define how the RSA key pair is generated; the definition is implementation. The evaluation does not cover the assessment of the strength of the keys generated, ONLY that a correct RSA key pair is generated. No assessment of the strength of the key pair will be performed. The SSLv3 standard allows for the TOE to operate in accordance with previous SSL standards when communicating with clients that are not SSLv3 capable.*

5.3.10 FCS_CKM.2 (SSL 1) Cryptographic key distribution

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA encrypted exchange of session keys for SSL handshake] that meet the following: [SSLv3 standard].

Application note: *This requirement is intended for SSL client and server authentication.*

5.3.11 FCS_CKM.2 (SSL 2) Cryptographic key distribution

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [digital certificates for public RSA keys] that meet the following: [certificate format given in X.509v3].

5.3.12 FCS_COP.1 (SSL 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 [digital signature generation and verification] in accordance with a specified cryptographic algorithm [RSA or AES] and cryptographic key sizes [1024 bits or smaller key sizes (RSA), 256 bits or smaller key sizes (AES) required for SSLv3 non-capable clients] that meet the following: [SSLv3 standard].

Application note: *The SSLv3 standard allows for the TOE to operate in accordance with previous SSL standards when communicating with clients that are not SSLv3 capable.*

5.3.12.1 FCS_COP.1 (SSL 2) Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1.1 The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [RC4, DES, Triple DES, or AES] and cryptographic key sizes [56 bit, 128 bit, 168 bit, or 256 bit] that meet the following: [SSLv3 standard].

Application note: *The SSLv3 standard allows for the TOE to operate in accordance with previous SSL standards when communicating with clients that are not SSLv3 capable.*

5.3.12.2 FCS_COP.1 (SSL 3) Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1.1 The TSF shall perform [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [MD5 or SHA1] and cryptographic key sizes [N/A] that meet the following: [SSLv3 standard].

Application note: *The SSLv3 standard allows for the TOE to operate in accordance with previous SSL standards when communicating with clients that are not SSLv3 capable.*

5.3.13 FCS_CKM.1 (IPSEC) Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple Data Encryption Standard (3DES-EDE)] and specified cryptographic key sizes [3 unique 56-bit keys] that meet the following: [NIST 800-67].

5.3.14 FCS_COP.1 (IPSEC 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 [

a) IPSec Security Association data encryption/decryption specified by IKE in RFC2409 as defined in TSP_IPSEC; and

b) IPSec ESP bulk data encryption/decryption specified by IKE in RFC2406 as defined in the TSP_IPSEC]

in accordance with a specified cryptographic algorithm [3DES-EDE] and cryptographic key sizes [168 bits] that meet the following: [NIST 800-67].

5.3.15 FCS_COP.1 (IPSEC 2) 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 [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [SHA-1 and MD5] and cryptographic key sizes [N/A] that meet the following: [FIPS-180-2 and RFC1321].

5.3.16 FCS_CKM.1 (SNMP) Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES] and specified cryptographic key sizes [64 bit] that meet the following: [generation of keys as defined in the SNMPv3 standard with the cipher suites defined in FCS_COP.1 (SNMP 2)].

5.3.17 FCS_COP.1 (SNMP 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 [hashing and verification] in accordance with a specified cryptographic algorithm [HMAC – SHA1] and cryptographic key sizes [none] that meet the following: [SNMPv3 standard].

5.3.18 FCS_COP.1 (SNMP 2) 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 [encryption and decryption] in accordance with a specified cryptographic algorithm [DES] and cryptographic key sizes [64-bit] that meet the following: [SNMPv3 standard].

5.3.19 FCS_CKM.1 (UDE) Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [192 bit] that meet the following: [none].

5.3.20 FCS_COP.1 (UDE) 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 [encryptions and decryption] **on user data stored on the HDDs** in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [192 bit] that meet the following: [none].

5.3.21 FCS_CKM.4 Cryptographic key destruction

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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [semiconductor memory state loss at power-down, semiconductor memory zeroization at power-up] that meets the following: [None].

5.3.22 Class FDP: User data protection

5.3.23 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [PrivUserAccess SFP] on [

- Subjects: authorized users;
- Object: functions accessible via WebUI and Local UI;
- Operations: access management interfaces].

5.3.24 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [PrivUserAccess SFP] to objects based on the following: [

- Subjects: Authorized users – role;
- Objects: functions accessible via WebUI and Local UI – role].

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

Authorized user(s) in System Administrator role will be granted access to the TOE security relevant functions accessible via the management interfaces].

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [no denial of access rules].

5.3.25 FDP_IFC.1 (IOW) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [User Data Protection Policy [TSP_IOW)] on [

- subjects: the hard disk drives
- information: image information
- operations: storage and erase of the image information].

5.3.26 FDP_IFF.1 (IOW) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] based on the following types of subject and information security attributes: [

- MFD Job
    - Type of the job (copy (landscape/stapled type only); print; workflow scan; scan-to-email; FAX; “Copy/Print, Store and Reprint”)
- Image information of the job
    - No security attributes].

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

- A MFD job of the type copy (landscape/stapled type only), print, workflow scan, fax, LanFax or scan-to-email may store image information in the reserved space on the hard disk drives.

- A MFD job of the type “Copy/Print, Store and Reprint” may store image information in a reserved space of the hard disk drive for the purpose of being reprinted at a later time].

FDP_IFF.1.3 The TSF shall enforce the [following additional information flow control SFP rules

- When the TOE is turned back on after a power failure, all temporary document image data stored on the hard disks of abnormally terminated jobs shall be overwritten according to DoD 5200.28-M.
- Once the system administrator has invoked standard ODIO, the space on the hard disk drives reserved for temporary and stored document image data shall be overwritten according to DoD 5200.28-M until the complete space is erased.
- Once the system administrator has invoked a full ODIO, the space on the hard disk drives reserved for temporary and stored document image (including stored “Copy/Print, Store and Reprint” jobs) and directory data, the Fax mailboxes, and the fax dial directory shall be overwritten according to DoD 5200.28-M until the complete space is erased.

].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none]

5.3.27 FDP_IFC.1 (FLOW) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [information flow control policy TSP_FLOW] on [

- subjects: the copy controller, the network controller, the FAX board
- information: fax image information and job data, command messages

- operations: receiving a fax, sending command messages, receiving command messages, copy operation of FAX image data, sending a FAX].

5.3.28 FDP_IFF.1 (FLOW) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [information flow control policy TSP_FLOW] based on the following types of subject and information security attributes: [

- the copy controller
  - copy operation from/to the shared memory area of the FAX board in progress or not
- the network controller
  - no security attributes
- the FAX board
  - PSTN port in use or not
- fax image information and job data
  - address of the memory where the data is stored (on the copy controller or on the FAX board)
- command messages
  - Type of the command message between FAX board and copy controller

].

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

- The copy controller is allowed to copy fax image information and job data from the shared memory of the FAX board to its own memory.
- The copy controller is allowed to copy fax image information and job data from its own memory to the shared memory of the FAX board.
- The FAX board is allowed to send out a fax over PSTN once the copy controller has signaled the end of the copy operation to the shared memory area.

- The FAX board is allowed to signal the copy controller “Fax received” once the PSTN connection has been terminated.
- The network controller is allowed to send image information and respective commands to the copy controller.]

].

FDP_IFF.1.3 The TSF shall enforce [the following additional information flow control SFP rules

- The FAX board is allowed to send command messages to the copy controller.
- The copy controller is allowed to send command messages to the FAX board.]

].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- The copy controller is not allowed to send fax image information to the network controller].

5.3.29 FDP_IFC.1 (FILTER) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

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

5.3.30 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 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 Package
  - Source IP address, protocol used (TCP or UDP), destination TCP or UDP port].

FDP_IFF.1.2 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 The TSF shall enforce the [implicit allow if no rules have been defined].

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

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes].

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 and protocols (either TCP or UDP) will be a match for allowed traffic.*

5.3.31 FDP_IFC.1 (IPSEC) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [IPSec SFP] on [

- Subjects: Printing clients;
- Information: All IP-based traffic to/from that destination/source;
- Operations: Printing].

5.3.32 FDP_IFF.1 (IPSEC) 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 The TSF shall enforce the [IPSec SFP] based on the following types of subject and information security attributes: [

- Subjects: Printing clients
  - IP address;
- Information: Print jobs
  - Issuer (printing client) of this print job].

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

- Printing clients initiate the establishment of a security association with the MFD
- The MFD establishes a security association with the printing client using IPSec "tunnel mode"
- All print jobs to the TOE must pass through the IPSec tunnel].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.5 The TSF shall explicitly deny any information flow based on the following rules: [none].

5.3.33 FDP_IFC.1 (SSL) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [SSLSec SFP] on [

- Subjects: Web clients;
- Information: All web-based traffic to/from that client;
- Operations: receiving HTTP traffic].

5.3.34 FDP_IFF.1 (SSL) 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 The TSF shall enforce the [SSLSec SFP] based on the following types of subject and information security attributes: [

- Subjects: web clients and servers
  - IP address and/or DNS name
- Information: X.509 certificates
  - RSA public and private keys; IP address or DNS name of the owner of the certificate].

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

- SSL session establishment and maintenance are in accordance with the SSLv3 standard.
- The SSL cryptographic operations are in accordance with the SSLv3 standard.
- The signature on the X.509 certificate received by the MFD is valid].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.5 The TSF shall explicitly deny any information flow based on the following rules: [HTTP traffic without an SSL tunnel].

5.3.35 FDP_IFC.1 (SNMP) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [SNMPSec SFP] on [

- Subjects: SNMP managers;
- Information: All SNMP traffic to/from that SNMP manager;
- Operations: receiving SNMP commands, sending SNMP packages/traps].

5.3.36 FDP_IFF.1 (SNMP) 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 The TSF shall enforce the [SNMPSec SFP] based on the following types of subject and information security attributes: [

- Subjects: SNMP managers
  - None;
- Information: SNMP message
  - Timeliness value, authentication data in SNMP message].

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

- Inbound SNMP messages comply with the SNMPv3 standard,;
- Authentication data in inbound SNMP packages is correct;
- Timeliness of the SNMP message is positively identified;
- Outbound messages must be encrypted].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.5 The TSF shall explicitly deny any information flow based on the following rules: [no additional rules based on security attributes that explicitly deny information flows].

5.3.37 FDP_RIP.1 (IOW 1) Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of **temporary image files will be overwritten according to DoD 5200.28-M** upon the *deallocation of the **temporary image files** from* the following objects: [copy (landscape/stapled type only), print, fax, network scan or scan to e-mail job].

Application Note: *This SFR shall ensure that all stored document image data written to the hard disk drive will be overwritten using the DoD 5200.28-M algorithm once the respective print, fax, workflow scan or scan-to-email job has completed or is deleted.*

5.3.38 FDP_RIP.1 (IOW 2) Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of **stored image files will be overwritten according to DoD 5200.28-M** upon the *deallocation of the* ***stored image files*** *from* the following objects: [stored "Copy/Print, Store and Reprint" jobs].

Application Note: *This SFR shall ensure that all stored document image data written to the hard disk drive will be overwritten using the DoD 5200.28-M algorithm once the respective "Copy/Print, Store and Reprint" job is deleted.*

5.3.39 FDP_UCT.1 (IPSEC) Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [IPSec SFP] to be able to *transmit and receive* user data in a manner protected from unauthorised disclosure.

5.3.40 FDP_UIT.1 (IPSEC) Data exchange integrity

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the [IPSec SFP] to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and/or replay* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.

5.3.41 FDP_UCT.1 (SSL) Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [SSLSec SFP] to be able to *transmit and receive* user data in a manner protected from unauthorised disclosure.

5.3.42 FDP_UIT.1 (SSL) Data exchange integrity

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the [SSLSec SFP] to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and/or replay* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.

5.3.43 FDP_UCT.1 (SNMP) Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [SNMPSec SFP] to be able to *transmit and receive* **management** data in a manner protected from unauthorized disclosure.

5.3.44 FDP_UIT.1 (SNMP) Data exchange integrity

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the [SNMPSec SFP] to be able to *transmit and receive* **management** data in a manner protected from *modification, deletion, insertion, and/or replay* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of **management** data, whether *modification, deletion, insertion, and/or replay* has occurred.

5.3.45 Class FIA: Identification and authentication

5.3.46 FIA_AFL.1 (AUT 1) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [authentication at the local user interface].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [lockout the SA login for a period of 3 minutes on the Local User Interface].

5.3.47 FIA_AFL.1 (AUT 2) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*1*] unsuccessful authentication attempt occurs related to [authentication at the Web User Interface from one particular Browser session].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [send the "401 Unauthorized" HTTP error code to this Browser session].

5.3.48 FIA_UAU.2 User authentication before any other action

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **system administrator or user** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **system administrator or user**.

5.3.49 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 **system administrator** while the authentication is in progress.

5.3.50 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **system administrator or user** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **system administrator or user**.

5.3.51 Class FMT: Security management

5.3.52 FMT_MOF.1 (FMT 1) Management of security functions behavior

Hierarchical to: No other components

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

FMT_MOF.1.1 The TSF shall restrict the ability to *disable and enable* the functions [

- Immediate Image Overwrite (IIO),
- On Demand Image Overwrite (ODIO),
- Network Authentication
- Audit Logging
- SSL
- IP Filtering
- IPSec
- SNMPv3
- IPv6

to [the system administrator].

5.3.53 FMT_MOF.1 (FMT 2) Management of security functions behavior

Hierarchical to: No other components

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

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of disable, enable and/or modify the behaviour* the functions [

- Change PIN,
- Invoke ODIO,
- Configure network authentication
- Assign authorization privileges to users,
- Establish IP address filtering rules,
- Create/install X.509 certificates,
- Create/install IPSec shared secrets,
- Create/install SNMPv3 shared secrets
- Download the audit log
- Configure IPv6]

to [the system administrator].

5.3.54 FMT_MSA.1 (IOW) Management of security attributes

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 The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] to restrict the ability to *change default, modify, delete [all security attributes]* to [nobody].

5.3.55 FMT_MSA.1 (FLOW) Management of security attributes

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 The TSF shall enforce the [information flow control policy TSP_FLOW] to restrict the ability to *change default, query, modify, delete [all security attributes]* to [nobody].

5.3.55.1 FMT_MSA.1 (SSL) Management of security attributes

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 The TSF shall enforce the [SSLSec SFP (TSP_SSL)] to restrict the ability to *[enable or disable]* the security attributes [SSL] to [the system administrator].

5.3.55.2 FMT_MSA.1 (FILTER) Management of security attributes

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 The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] to restrict the ability to *query, modify, delete* the security attributes [source address] to [they system administrator].

5.3.55.3 FMT_MSA.1 (IPSEC) Management of security attributes

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	The TSF shall enforce the [IPSec SFP (TSP_IPSEC)] to restrict the ability to *[enable or disable]* the security attributes [IPSEC] to [the system administrator].

5.3.55.4 FMT_MSA.1 (SNMP) Management of security attributes

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	The TSF shall enforce the [SNMPSec SFP (TSP_SNMP)] to restrict the ability *[enable or disable]* the security attributes [SNMP] to [the system administrator].

5.3.56 FMT_MSA.3 (IOW) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: *FMT_MSA.1 (IOW) and FMT_MSA.3 (IOW) require the static initialization of the security attribute "Possible types of MFD jobs". The TOE itself shall be able to initialize and manage this security attribute, so nobody shall be able to modify these values.*

5.3.57 FMT_MSA.3 (FLOW) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles

FMT_MSA.3.1	The TSF shall enforce the [information flow control policy TSP_FLOW] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: *FMT_MSA.1 (FLOW) and FMT_MSA.3 (FLOW) require the static initialization of the security attributes "Types of Command Messages between FAX board and copy controller", and the address spaces of these two objects. The TOE itself shall be able to initialize and manage these security attributes, so nobody shall be able to modify these values.*

5.3.57.1 FMT_MSA.3 (SSL) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [SSLSec SFP] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.1 (SSL) and FMT_MSA.3 (SSL) apply to the SSL function. The only configuration option available for SSL is the ability to enable or disable it. While the system administrator can enable or disable SSL, doing so does not change or override default or initial values associated with object creation.

5.3.57.2 FMT_MSA.3 (FILTER) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1	The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.1 (FILTER) and FMT_MSA.3 (FILTER) apply to the IP Filter function. The default configuration is permissive (all hosts can connect to the TOE). While the system administrator can configure a restrictive list of hosts that can connect to the TOE (with those hosts not listed unable to connect to the TOE), entering a source address into the list does not change or override default or initial values associated with object creation.

5.3.57.3 FMT_MSA.3 (IPSEC) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [IPSec SFP (TSP_IPSEC)] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.1 (IPSEC) and FMT_MSA.3 (IPSEC) apply to the IPSec function. The default configuration is permissive (IPSec is turned off). While the system administrator can enable IPSec so that hosts can connect to the TOE over an encrypted connection, enabling IPSec does not change or override default or initial values associated with object creation.

5.3.57.4 FMT_MSA.3 (SNMP) Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [SNMPSec SFP (TSP_SNMP)] to provide _permissive_ default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: FMT_MSA.1 (SNMP) and FMT_MSA.3 (SNMP) apply to the SNMP function. The default configuration is permissive (SNMP is turned off). While the system administrator can enable SNMP, enabling SNMP does not change or override default or initial values associated with object creation.

5.3.58 FMT_MTD.1 (AUT) Management of TSF data

Hierarchical to: No other components

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

FMT_MTD.1.1 The TSF shall restrict the ability to [_create_, _read (download)_] the [

- Audit log]

to [the system administrator].

5.3.59 FMT_MTD.1 (SNMP) Management of TSF data

Hierarchical to: No other components

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

FMT_MTD.1.1 The TSF shall restrict the ability to _delete_, [_create_] the [

- SNMPv3 authentication key,
- SNMPv3 privacy key,
- X.509 Server certificate]

to [the system administrator].

5.3.60 FMT_MTD.1 (FILTER) Management of TSF data

Hierarchical to: No other components

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

FMT_MTD.1.1 The TSF shall restrict the ability to _modify_, _delete_, [_create_] the [

- IP filter rules]

to [the system administrator].

5.3.61 FMT_SMF.1 Specification of Management Functions

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] (Local User Interfaces);
- Enable/disable On Demand Image Overwrite (ODIO) [TSF_IOW] (Local User Interfaces);
- Change PIN (Web and Local User Interfaces);
- Invoke ODIO [TSF_IOW] (Web and Local User Interfaces);
- Create a recurrence schedule for “On Demand” image overwrite (Web User Interface);
- Enable/disable audit function (Web User Interface);
- Transfer the audit records (if audit is enabled) to a remote trusted IT product (Web User Interface);
- Enable/disable SSL (Web User Interface);
- Create/upload/download X.509 certificates (Web User Interface);
- Enable/disable and configure IPSec tunneling (Web User Interface);
- Disable IPSec tunneling (Local User Interface);
- Enable/disable and configure SNMPv3 (Web User Interface);
- Enable/disable and configure (specify the IP address and/or IP address range for remote trusted IT products (presumed) allowed to connect to the TOE via the network interface) IP filtering] (Web User Interface);
- Enable/disable and configure IPv6 (Web User Interface);
- Enable/disable and configure Disk Encryption (Web User Interface);

- Configure network authentication (Web User Interface);
- Configure device authorization (Web User Interface)].

5.3.62 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [system administrator, 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. Any authorized human or IT user who has not been explicitly assigned the "system administrator" role is granted the "user" role.*

5.3.63 Class FPR: Privacy

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

5.3.64 Class FPT: Protection of the TSF

5.3.65 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3.66 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *<u>during initial start-up</u>* to demonstrate the correct operation of *<u>the TSF</u>*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *<u>TSF data</u>*.

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

5.3.67 Class FRU: Resource utilization

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

5.3.68 Class FTA: TOE access

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

5.3.69 Class FTP: Trusted paths/channels

5.3.70 FTP_ITC.1 Inter-TSF trusted channel

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 user document data, user function data, and TSF data over any Shared-medium interface].

5.3.71 FTP_TRP.1 (IPSEC) Trusted path (NOTE: IPSec SFP)

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*.

FTP_TRP.1.2 The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require use of the trusted path for [

- *All IP-based traffic to or from that destination or source*].

5.3.72 FTP_TRP.1 (SSL) Trusted path (NOTE: SSLSec SFP)

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*.

FTP_TRP.1.2 The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require use of the trusted path for [

- *Print jobs and LanFax jobs submitted via Web UI,*
- *The security management functions available to the system administrator from the Web UI*].

5.3.73 FTP_TRP.1 (SNMP) Trusted path (NOTE: SNMPSec SFP)

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*.

FTP_TRP.1.2 The TSF shall permit *remote users and the TSF* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require use of the trusted path for [*SNMP messages*].

5.4 TOE Security Assurance Requirements

Table 15 lists the security assurance requirements for an EAL3+ augmented with ALC_FLR.3 evaluation. This Security Target claims conformance with these Security Assurance Requirements; they are not iterated or refined from their counterparts in CC Part 3.

Table 15: Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Assurance Class	Assurance Components
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Flaw reporting procedures (augmentation of EAL3)
	ALC_LCD.1 Developer defined life-cycle model
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.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.5 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

5.6 Rationale for Security Functional Requirements

Table 16 and
Table 17 below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE.

Table 16: Completeness of Security Functional Requirements

SFRS	OBJECTIVES

	O.AUDITS	O.RECOVER	O.FAXLINE	O.MANAGE	O.CONTROL_ACCESS	O.PROTECT_COM
FAU_GEN.1	X			X		
FAU_SAR.1	X			X		
FAU_SAR.2	X			X		
FAU_STG.1	X					
FAU_STG.4	X					
FCS_CKM.1 (SSL 1)						X
FCS_CKM.1 (SSL 2)						X
FCS_CKM.2 (SSL 1)						X
FCS_CKM.2 (SSL 2)						X
FCS_COP.1 (SSL 1)						X
FCS_COP.1 (SSL 2)						X
FCS_COP.1 (SSL 3)						X
FCS_CKM.1 (IPSEC)						X
FCS_COP.1 (IPSEC 1)						X
FCS_COP.1 (IPSEC 2)						X
FCS_CKM.1 (SNMP)						X
FCS_COP.1 (SNMP 1)						X
FCS_COP.1 (SNMP 2)						X
FCS_CKM.1 (UDE)		X				
FCS_COP.1 (UDE)		X				
FCS_CKM.4						X
FDP_ACC.1						X
FDP_ACF.1						X
FDP_IFC.1 (IOW)		X				
FDP_IFF.1 (IOW)		X				
FDP_IFC.1 (FLOW)		X	X			
FDP_IFF.1 (FLOW)		X	X			
FDP_IFC.1 (FILTER)					X	X
FDP_IFF.1 (FILTER)					X	X
FDP_IFC.1 (IPSEC)					X	X
FDP_IFF.1 (IPSEC)					X	X
FDP_IFC.1 (SSL)					X	X
FDP_IFF.1 (SSL)					X	X
FDP_IFC.1 (SNMP)					X	X

	OBJECTIVES					
SFRS	O.AUDITS	O.RECOVER	O.FAXLINE	O.MANAGE	O.CONTROL_ACCESS	O.PROTECT_COM
FDP_IFF.1 (SNMP)					X	X
FDP_RIP.1 (IOW 1)		X				
FDP_RIP.1 (IOW 2)		X				
FDP_UCT.1 (IPSEC)						X
FDP_UIT.1 (IPSEC)						X
FDP_UCT.1 (SSL)						X
FDP_UIT.1 (SSL)						X
FDP_UCT.1 (SNMP)						X
FDP_UIT.1 (SNMP)						X
FIA_AFL.1 (AUT 1)				X		
FIA_AFL.1 (AUT 2)				X		
FIA_UAU.2				X		
FIA_UAU.7				X		
FIA_UID.2				X		
FMT_MOF.1 (FMT 1)		X		X		
FMT_MOF.1 (FMT 2)		X		X		
FMT_MSA.1 (IOW)		X				
FMT_MSA.1 (FLOW)			X			
FMT_MSA.1 (FILTER)					X	X
FMT_MSA.1 (SSL)					X	X
FMT_MSA.1 (IPSEC)					X	X
FMT_MSA.1 (SNMP)					X	X
FMT_MSA.3 (IOW)		X				
FMT_MSA.3 (FLOW)			X			
FMT_MSA.3 (FILTER)					X	X
FMT_MSA.3 (SSL)					X	X
FMT_MSA.3 (IPSEC)					X	X
FMT_MSA.3 (SNMP)					X	X
FMT_MTD.1 (AUT)	X			X		
FMT_MTD.1 (FILTER)				X	X	X
FMT_MTD.1 (SNMP)				X	X	X
FMT_SMF.1		X		X		X
FMT_SMR.1		X		X		

SFRS	OBJECTIVES					
	O.AUDITS	O.RECOVER	O.FAXLINE	O.MANAGE	O.CONTROL_ACCESS	O.PROTECT_COM
FPT_STM.1	X					
FPT_TST.1				X		X
FTP_ITC.1				X		
FTP_TRP.1 (IPSEC)				X		
FTP_TRP.1 (SSL)				X		
FTP_TRP.1 (SNMP)				X		

Table 17: Sufficiency of Security Functional Requirements

Objective	Rationale
O.AUDITS	FAU_GEN.1 ensures that the TOE is able to generate time-stamped audit records of a specified set of security-relevant events related to TOE operations. FAU_SAR.1 and FAU_SAR.2 ensure that the TOE is able to make available only to users granted explicit “read” access (TOE administrators) audit information in a form suitable for viewing and evaluation/analysis. FAU_STG.1 and FAU_STG.4 ensure that the TOE is able to prevent unauthorized modification of audit trail records and, when the audit trail file is full, is able to overwrite the oldest stored audit records without other modification to stored records. FMT_MTD.1 (AUT) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to clear, delete, create, read and download the audit log. FPT_STM.1 ensures that the TOE provides a reliable timestamp for inclusion in the audit log.

Objective	Rationale
O.RECOVER	FCS_CKM.1 (UDE) and FCS_COP.1 (UDE) ensure that the TOE provides the cryptographic support and services, secure hashing and associated key management capabilities necessary to encrypt user data that is committed to the hard drive so that it cannot be recoved in plaintext. FDP_IFF.1 (IOW) together with FDP_IFC.1 (IOW) ensures that all temporary document image data of abnormally terminated jobs will be overwritten once the TOE is turned back on after a power failure. Additionally, these two requirements ensure that the complete space reserved for temporary document image data can be overwritten "on demand" by the system administrator. FDP_IFF.1 (FLOW) and FDP_IFC.1 (FLOW) ensure that Fax jobs will not be written to the HDD at all. FDP_RIP.1 (IOW 1) and FDP_RIP.1 (IOW 2) ensure that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing. FMT_MOF.1 (FMT 1) and FMT_MOF.1 (FMT 2) restrict the access to this function to the system administrator. FMT_MSA.1 (IOW) and FMT_MSA.3 (IOW) define the space where the temporary document image data can be stored and deny the modification of this space by anyone. FMT_SMF.1 requires that there is a possibility to invoke this ODIO function. FMT_SMR.1 ensures that the TOE maintains the system administrator role – a trusted individual who can administer the TOE.
O.FAXLINE	FDP_IFC.1 (FLOW) and FDP_IFF.1 (FLOW) define the rules according to which an information flow between network controller, copy controller and FAX board (if installed) is allowed. By implementing a store-and-forward principle in both directions, a direct interconnection between the PSTN and the internal network is not possible.

Objective	Rationale
	FMT_MSA.1 (FLOW) and FMT_MSA.3 (FLOW) define the possible command types and the address spaces of the copy controller and the FAX board. Nobody shall be able to modify these parameters.
O.MANAGE	FAU_GEN.1 ensures that the TOE is able to generate time-stamped audit records of a specified set of security-relevant events related to TOE operations. FAU_SAR.1 and FAU_SAR.2 ensure that the TOE is able to make available only to users granted explicit “read” access (TOE administrators) audit information in a form suitable for viewing and evaluation/analysis. FIA_AFL.1 (AUT 1) ensures that the TOE takes specific and immediate self-protection action when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Local User Interface. FIA_AFL.1 (AUT 2) provides an appropriate error message to the users’ web browser when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Web User Interface. Self-protection of the TOE is not possible due to the properties of a web interface (no dependable identification of the user’s terminal and therefore no possibility to lock this terminal). FIA_UAU.2 and FIA_UID.2 ensure that system administrators are authenticated (and implicitly identified) before accessing the security functionality of the TOE. FIA_UAU.7 ensures that only obscured feedback generated by the authentication process is provided to system administrators before successful authentication. FMT_MOF.1 (FMT 1) and FMT_MOF.1 (FMT 2) restrict the access to these management functions to the system administrator. FMT_MTD.1 (AUT) ensures that users of the system cannot modify the audit log.

Objective	Rationale
	FMT_MTD.1 (FILTER) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to create or delete the X.509 Server certificate. FMT_MTD.1 (SNMP) ensures that only system administrators can modify the SNMPv3 security properties (authentication key, privacy key, server certificate). FMT_SMF.1 ensures that the security management functions (i.e., enable/disable IIO and ODIO, change system administrator PIN, and invoke/abort ODIO) are available on the TOE. FMT_SMR.1 manages the role "system administrator". FPT_TST.1 ensures that the TOE tests its security functions so that the system administrator will know if they are not working properly. FTP_ITC.1, FTP_TRP.1 (IPSEC), FTP_TRP.1 (SSL), and FTP_TRP.1 (SNMP) ensure that the TOE provides communications channels between itself and remote trusted IT products and remote users distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
O.CONTROL_ACCESS	FDP_IFC.1 (FILTER), FDP_IFC.1 (IPSEC), FDP_IFC.1 (SSL), FDP_IFC.1 (SNMP), FDP_IFF.1(FILTER), FDP_IFF.1 (IPSEC), FDP_IFF.1 (SSL), and FDP_IFF.1 (SNMP) ensure that the IP_Filter SFP is enforced to control and protect information flow between controlled subjects (IP address) based on specific subject and information security attributes to enable the transmission and receipt of user or management data in a protected manner. FMT_MSA.1 (FILTER), FMT_MSA.1 (SSL), FMT_MSA.1 (IPSEC), FMT_MSA.1 (SNMP), FMT_MSA.3 (FILTER), FMT_MSA.3 (SSL), FMT_MSA.3 (IPSEC) and FMT_MSA.3 (SNMP) define the possible actions that a system administrator can take concerning IP Filter, SSL, IPSec and SNMP. FMT_MTD.1 (FILTER) and FMT_MTD.1 (SNMP) ensure that the TOE enforces policies so that only system administrators

Objective	Rationale
	have the capability to and query, modify, delete or create the IP filter rules or modify SNMP security attributes (keys and certificates).
O.PROTECT_COM	FCS_CKM.1 (SSL 1), FCS_CKM.1 (SSL 2) FCS_CKM.1 (IPSEC), FCS_CKM.1 (SNMP), FCS_CKM.2 (SSL 1), FCS_CKM.2 (SSL 2), FCS_CKM.4, FCS_COP.1 (SSL 1), FCS_COP.1 (SSL 2), FCS_COP.1 (SSL 3), FCS_COP.1 (IPSEC 1), FCS_COP.1 (IPSEC 2), FCS_COP.1 (SNMP 1) and FCS_COP.1 (SNMP 2) ensure that the TOE provides the cryptographic support and services, secure hashing and associated key management capabilities necessary to assure secure communication between TOE components and remote trusted products by using specified cryptographic key generation algorithms and associated cryptographic key distribution and destruction methods. FDP_ACC.1 and FDP_ACF.1 ensure that the TOE enforces the PrivUserAccess SFP on subjects, objects, information, and operations and applies specific rules on all operations involving controlled subjects and objects, limiting access to management interfaces to the System Administrator. FDP_IFC.1 (FILTER), FDP_IFC.1 (IPSEC), FDP_IFC.1 (SSL), FDP_IFC.1 (SNMP), FDP_IFF.1 (FILTER), FDP_IFF.1 (IPSEC), FDP_IFF.1 (SSL), FDP_IFF.1 (SNMP), FDP_UCT.1 (IPSEC), FDP_UCT.1 (SSL), FDP_UCT.1 (SNMP), FDP_UIT.1 (IPSEC), FDP_UIT.1 (SSL), and FDP_UIT.1 (SNMP) ensure that the policies are enforced to control and protect information flow between controlled subjects (IP address) based on specific subject and information security attributes to enable the transmission and receipt of user or management data in a protected manner and the protection and removal of residual user data from a controlled resource. FMT_MSA.1 (FILTER), FMT_MSA.1 (SSL), FMT_MSA.1 (IPSEC), FMT_MSA.1 (SNMP), FMT_MSA.3 (FILTER), FMT_MSA.3 (SSL), FMT_MSA.3 (IPSEC) and FMT_MSA.3 (SNMP) define the possible actions that a system administrator can take concerning IP Filter, SSL, IPSec and SNMP. FMT_MTD.1 (FILTER) and FMT_MTD.1 (SNMP) ensure that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to create or delete X.509 Server certificates.

Objective	Rationale
	FMT_SMF.1 ensures that the security management functions (i.e., enable/disable SSL, enable/disable IPSec, etc) are available on the TOE. FPT_TST.1 ensures that the TOE's communication security features are working properly.

5.7 Rationale for Security Assurance Requirements

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 3 is appropriate.

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.

5.8 Rationale for Dependencies

5.8.1 Security Functional Requirement Dependencies

Table 18 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 18: SFR Dependencies Satisfied

Functional Component ID	Dependency (ies)	Satisfied
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_CKM.1 (SSL 1)	FCS_CKM.2 or	Yes, FCS_CKM.2(SSL 1), FCS_CKM.2 (SSL 2) and

Functional Component ID	Dependency (ies)	Satisfied
	FCS_COP.1	FCS_COP.1 (SSL 2)
	FCS_CKM.4	Yes
FCS_CKM.1 (SSL 2)	FCS_CKM.2 or FCS_COP.1	Yes, FCS_CKM.2(SSL 2), FCS_CKM.2 (SSL 1) and FCS_COP.1 (SSL 1)
	FCS_CKM.4	Yes
FCS_CKM.2 (SSL 1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SSL 1)
	FCS_CKM.4	Yes
FCS_CKM.2 (SSL 2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SSL 2)
	FCS_CKM.4	Yes
FCS_COP.1 (SSL 1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SSL 1)
	FCS_CKM.4	Yes
FCS_COP.1 (SSL 2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SSL 2)
	FCS_CKM.4	Yes
FCS_COP.1 (SSL 3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes FCS_CKM.1 (SSL 1) and FCS_CKM.1 (SSL 2)
	FCS_CKM.4	Yes
FCS_CKM.1 (IPSEC)	FCS_CKM.2 or FCS_COP.1	Yes, FCS_COP.1 (IPSEC 1)
	FCS_CKM.4	Yes
FCS_COP.1 (IPSEC 1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (IPSEC)
	FCS_CKM.4	Yes
FCS_COP.1 (IPSEC 2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (IPSEC)
	FCS_CKM.4	Yes
FCS_CKM.1 (SNMP)	FCS_CKM.2 or FCS_COP.1	Yes, FCS_COP.1 (SNMP 1), FCS_COP.1 (SNMP 2)
	FCS_CKM.4	Yes
FCS_COP.1 (SNMP 1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SNMP)
	FCS_CKM.4	Yes
FCS_COP.1 (SNMP 2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (SNMP)
	FCS_CKM.4	Yes
FCS_CKM.1 (UDE)	FCS_CKM.2 or FCS_COP.1	Yes, FCS_COP.1 (UDE)
	FCS_CKM.4	Yes
FCS_COP.1 (UDE)	FDP_ITC.1 or	Yes, FCS_CKM.1 (UDE)

Functional Component ID	Dependency (ies)	Satisfied
	FDP_ITC.2 or FCS_CKM.1	
	FCS_CKM.4	Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, FCS_CKM.1 (all)
FDP_ACC.1	FDP_ACF.1	Yes, FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	Yes, FDP_ACC.1
	FMT_MSA.3	Yes, FMT_MSA.3
FDP_IFC.1 (IOW)	FDP_IFF.1	Yes, FDP_IFF.1 (IOW)
FDP_IFF.1 (IOW)	FDP_IFC.1	Yes, FDP_IFC.1 (IOW)
	FMT_MSA.3	Yes, FMT_MSA.3 (IOW)
FDP_IFC.1 (FLOW)	FDP_IFF.1	Yes, FDP_IFF.1 (FLOW)
FDP_IFF.1 (FLOW)	FDP_IFC.1	Yes, FDP_IFC.1 (FLOW)
	FMT_MSA.3	Yes, FMT_MSA.3 (FLOW)
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	Yes, FMT_MSA.3 (FILTER)
FDP_IFC.1 (IPSEC)	FDP_IFF.1	Yes, FDP_IFF.1 (IPSEC)
FDP_IFF.1 (IPSEC)	FDP_IFC.1	Yes, FDP_IFC.1 (IPSEC)
	FMT_MSA.3	Yes, FMT_MSA.3 (IPSEC)
FDP_IFC.1 (SSL)	FDP_IFF.1	Yes, FDP_IFF.1 (SSL)
FDP_IFF.1 (SSL)	FDP_IFC.1	Yes, FDP_IFC.1 (SSL)
	FMT_MSA.3	Yes, FMT_MSA.3 (SSL)
FDP_IFC.1 (SNMP)	FDP_IFF.1	Yes, FDP_IFF.1 (SNMP)
FDP_IFF.1 (SNMP)	FDP_IFC.1	Yes, FDP_IFC.1 (SNMP)
	FMT_MSA.3	Yes, FMT_MSA.3 (SNMP)
FDP_RIP.1 (IOW 1)	None	
FDP_RIP.1 (IOW 2)	None	
FDP_UCT.1 (IPSEC)	FDP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (IPSEC)
	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (IPSEC)
FDP_UCT.1 (SSL)	FTP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (SSL)
	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SSL)
FDP_UCT.1 (SNMP)	FTP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (SNMP)
	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SNMP)
FDP_UIT.1 (IPSEC)	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (IPSEC)
	FTP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (IPSEC)
FDP_UIT.1 (SSL)	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SSL)
	FTP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (SSL)
FDP_UIT.1 (SNMP)	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SNMP)
	FTP_ITC.1 or FTP_TRP.1	Yes, FTP_TRP.1 (SNMP)

Functional Component ID	Dependency (ies)	Satisfied
FIA_AFL.1 (AUT 1)	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_AFL.1 (AUT 2)	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_UAU.2	FIA_UID.1	Yes, hierarchically by FIA_UID.2
FIA_UAU.7	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_UID.2	None	
FMT_MOF.1 (FMT 1)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MOF.1 (FMT 2)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1 (IOW)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (IOW)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1 (FLOW)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (FLOW)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1 (FILTER)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (FILTER)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1 (IPSEC)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (IPSEC)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1 (SSL)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SSL)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.1 (SNMP)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (SNMP)
	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MSA.3 (IOW)	FMT_MSA.1	Yes, FMT_MSA.1 (IOW)
	FMT_SMR.1	Yes
FMT_MSA.3 (FLOW)	FMT_MSA.1	Yes, FMT_MSA.1 (FLOW)
	FMT_SMR.1	Yes
FMT_MSA.3 (FILTER)	FMT_MSA.1	Yes, FMT_MSA.1 (FILTER)
	FMT_SMR.1	Yes
FMT_MSA.3 (IPSEC)	FMT_MSA.1	Yes, FMT_MSA.1 (IPSEC)
	FMT_SMR.1	Yes
FMT_MSA.3 (SSL)	FMT_MSA.1	Yes, FMT_MSA.1 (SSL)
	FMT_SMR.1	Yes
FMT_MSA.3 (SNMP)	FMT_MSA.1	Yes, FMT_MSA.1 (SNMP)
	FMT_SMR.1	Yes
FMT_MTD.1 (AUT)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (FILTER)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (SNMP)	FMT_SMF.1	Yes

Functional Component ID	Dependency (ies)	Satisfied
	FMT_SMR.1	Yes
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Yes, hierarchically by FIA_UID.2
FPT_STM.1	None	
FPT_TST.1	None	
FTP_ITC.1	None	
FTP_TRP.1 (IPSEC)	None	
FTP_TRP.1 (SSL)	None	
FTP_TRP.1 (SNMP)	None	

5.8.2 Security Assurance Requirement Dependencies

SAR dependencies identified in the CC have been met by this ST as shown in Table 19.

Table 19: EAL3 (Augmented with ALC_FLR.3) SAR Dependencies Satisfied

Assurance Component ID	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	Yes, hierarchically
ADV_FSP.3	ADV_TDS.1	Yes, hierarchically
ADV_TDS.2	ADV_FSP.3	Yes
AGD_OPE.1	ADV_FSP.1	Yes, hierarchically
AGD_PRE.1	None	
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	Yes, hierarchically Yes Yes
ALC_CMS.3	None	
ALC_DEL.1	None	
ALC_DVS.1	None	
ALC_LCD.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	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	Yes Yes, hierarchically Yes, hierarchically
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes, hierarchically Yes
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	Yes Yes Yes
ATE_FUN.1	ATE_COV.1	Yes, hierarchically
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes, hierarchically Yes Yes Yes, hierarchically Yes
AVA_VAN.2	ADV_ARC.1 ADV_FSP.1 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	Yes Yes, hierarchically Yes, hierarchically Yes Yes

6 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.3).

- Image Overwrite (TSF_IOW)
- Information Flow (TSF_FLOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSEC)
- Network Management Security (TSF_NET_MGMT)
- Security Management (TSF_FMT)
- User Data Protection –AES (TSF_EXP_UDE)

6.1.1 Image Overwrite (TSF_IOW)

The TOE implements an image overwrite security function (IIO) to overwrite temporary files created during the copying (landscape/stapled type only), printing, network scan, or scan to e-mail process.

The main controller spools and processes documents to be copied (landscape/stapled type only), printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive of the main controller. 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 using a three pass overwrite procedure as described in DoD 5200.28-M.

User image files associated with the Copy/Print, Store and Reprint feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job using the 5200.28-M algorithm. The stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite. 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 all files that have been stored at the request of a user via Copy/Print, Store and Reprint jobs.

The image overwrite security function can also be invoked manually by the system administrator (ODIO). Once invoked, the ODIO cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section on the hard disk according to DoD 5200.28-M, and then the main controller reboots.

Once started, ODIO cannot be canceled.

If the TOE is turned back on after a power failure, the TOE automatically starts an IIO procedure for all abnormally terminated print or scan jobs prior to come "on line".

6.1.2 Information Flow (TSF_FLOW)

The TOE provides separation between the optional FAX board PSTN port and the main controller network port as illustrated in Figure 2: TSF_FLOW .

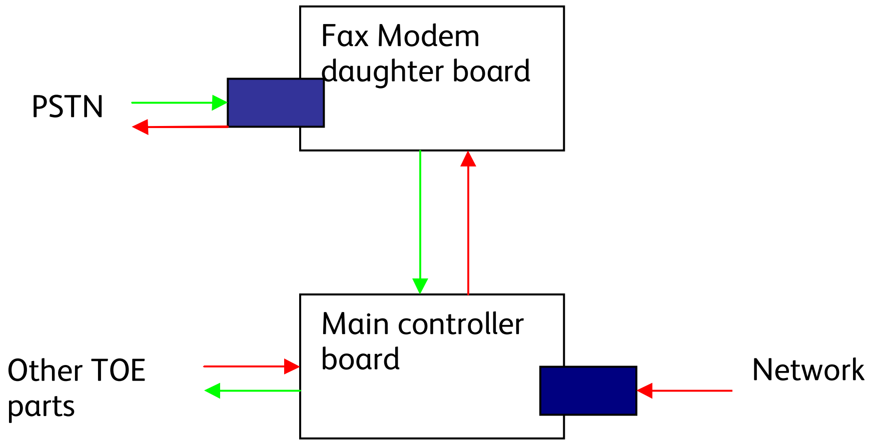

Figure 2: TSF_FLOW

The main controller software controls all of the functions of the main controller board as well as the FAX modem daughter board. There is a physical (electrical signal) interface between the two. Separation between the PSTN port on the FAX board and the network port on the main controller board is established through the architectural design of the main controller software.

For outgoing FAX from the scanner, the main controller will control the scanner to scan in all pages of the outgoing fax. Once the pages have been scanned into main controller board memory the main controller software will initiate the fax send function of the FAX board modem. The main controller will not initiate the activation of the PSTN port until the entire job has been scanned. For outgoing FAX from LanFax, the main controller will receive the entire job onto the HDD, render the job to a (compressed) bitmap, and then initiate the fax send function of the FAX board modem. The main controller will not initiate the activation of the PSTN port until the entire job has been received and rendered.

For incoming FAX the modem on the FAX board will signal a request for service from the main controller, which will initiate the fax receive function of the FAX board modem. The main controller software will buffer the entire incoming fax data into main controller board memory. Once the entire job has been received, the main controller software will control the modem to disconnect the call at the PSTN port. Subsequently the main controller software will initiate the marking function of the IOT software to produce hardcopy output.

6.1.3 Authentication (TSF_SYS_AUT)

The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions (see Section 6.1.4 - Network Authentication (TSF_NET_AUT)). While the system administrator is typing the PIN number, the TOE displays an asterisk for each character entered to hide the value entered. Identification of the system administrator at the Local User Interface is implicit -- the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window.

The authentication process will be delayed at the Local User Interface, for 3 minutes if 3 wrong PINs were entered in succession. If 1 wrong PIN is entered at the web interface from one particular Browser session, the TOE will send an error message (“HTTP 401 Unauthorized”) to this Browser session. It will be up to the browser whether to display the message to the user or to re-prompt for authentication.

6.1.4 Network Authentication (TSF_NET_AUT)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password which is then validated by the designated authentication server (a trusted remote IT entity). The user is not required to login to the network; the account is authenticated by the server as a valid user. The remote authentication services supported by the TOE are: LDAP v4, Kerberos v5 (Solaris), Kerberos v5 (Windows 2000/2003), and SMB (Windows NT.4x/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*.

Application Note: There is a difference between authentication and accounting (for a discussion see Application Note in Section 6.1.5 - Security Audit (TSF_FAU)). The TOE defines one user authentication method: Network Authentication.

6.1.5 Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., copy/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 system start-up/shutdown, ODIO start/completion, and copy, print, scan, email, local fax, I-Fax (not evaluated), and LanFax jobs. 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 Web UI screen contains a button labeled “Save as Text File” that is viewable by all users. If this button is selected, and the system administrator is not already logged in through the interface, then a system administrator login alert window is presented. Once the system administrator has successfully logged in, then the audit log file becomes downloadable.

Application Note: The device provides both authentication and accounting – both serve different functions. The TOE defines (see Guidance documentation) three accounting methods: *Auditron*, *Xerox Standard Accounting (XSA)*, and *Network Accounting*; these three methods are mutually exclusive.

The Guidance documentation defines only one user authentication method: *Network Authentication* (see Section 6.1.4 - Network Authentication (TSF_NET_AUT)). *Network Authentication* is mutually exclusive with *Auditron*, however, it can be enabled concurrently with *Network Accounting* and *XSA*.

The *Auditron* method utilizes a PIN-based identification system that is maintained in a database resident on the main controller board. The *XSA* method is also PIN-based, and its database is also resident on the main controller board. *Network Accounting* works with an external Accounting server (i.e., Equitrac or Control Systems). *Network Accounting* uses full character set IDs.

For network scan and email jobs the accounting IDs (i.e., PINS) required by the *XSA*, or *Network Accounting*, will be recorded in the audit log.

If *Network Authentication* is enabled, then the name required by *Network Authentication* will be recorded in the audit log. The Audit Log does not record anything for Auditron.

For print and LanFax jobs, the network username associated with the logged in user at the client workstation will be recorded in the audit log.

6.1.6 Cryptographic Support (TSF_FCS)

The TOE utilizes data encryption (AES, RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-186, AES -- FIPS-197, SSLv3, SNMPv3.

6.1.7 User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing. SSL must be enabled before setting up either IPSec, SNMPv3, or before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. The TOE creates and enforces the informal security policy model, "All communications to the Web server will utilize SSL (HTTPS)."

All information that is transmitted between the TOE and a remote trusted product using SSL is protected from both disclosure and modification. The disclosure protection is accomplished by the symmetric encryption of the data being transferred using the DES EDE (aka, Triple DES – defined in US FIPS-46-3) cipher and a per connection key generated as part of the SSLv3 protocol. The modification protection is accomplished by the use of the HMAC (Hashed Message Authentication Code – defined by IETF RFC2104) that is incorporated into the SSLv3 record transfer protocol.

Once SSL is enabled on the TOE web services requests from clients must be received through HTTPS.

Additionally, the TOE can act as a web client in the case of Network scanning. When acting as an SSL client to SSL scan repository, the TOE can validate the remote server's certificate against a trusted CA; in this configuration, if it cannot validate the identity of the certificate received from the remote server it will not communicate with the scan repository.

6.1.8 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 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.

6.1.9 User Data Protection – IPSec (TSF_FDP_IPSec)

The TOE implements the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE through the lpr and port 9100 network interfaces by encrypting all IP-based traffic through IPSec. Printing clients initiate the establishment of a security association with the MFD. The MFD establishes a security association with the printing client using IPSec "tunnel mode." Thereafter, all IP-based traffic to and from this destination will pass through the IPSec tunnel until either end powers down, or resets, after which the tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client.

IPSec secures packet flows through two protocols – Encapsulating Security Payload (ESP) and Authentication Header (AH). ESP provides authentication, data confidentiality and message integrity. The ESP extension header provides origin authenticity, integrity, and confidentiality of a packet. AH provides authentication and message integrity, but does not offer confidentiality. The AH guarantees connectionless integrity and data origin authentication of IP datagrams. IPSec also defines one key exchange protocol – Internet Key Exchange (IKE) protocol.

Note: The TOE cannot enforce the IPSec (TSF_FDP_IPSec) security function when it is configured for AppleTalk or IPX networks.

6.1.10 Network Management Security (TSF_NET_MGMT)

The TOE supports SNMPv3 as part of its security solution through the SNMPSec SFP. The SNMPv3 protocol is used to authenticate each SNMP message, as well as, provide encryption of the data as described in RFC 3414.

As implemented, both an authentication and privacy (encryption) password must be set up both at the device and at the manager. Both passwords must be a minimum of 8 characters. SNMP uses SHA-1 for authentication.

6.1.11 Security Management (TSF_FMT)

The TSF_FMT utilizes the front panel software module security mechanisms to allow only authenticated system administrators the capability to enable or disable the TSF_IOW function, change the system administrator PIN, or manually invoke "On Demand" Image Overwrite.

Additionally, TSF_FMT utilizes the web server authentication mechanism to allow only authenticated system administrators the capability to: manually invoke "On Demand" Image Overwrite; enable/disable the audit function; transfer the audit records (if audit is enabled) to a remote trusted IT product; enable/disable SSL; configure IPv6; configure network authentication; create/upload/download X.509 certificates; and enable/disable and configure (specify the IP address and/or IP address range (presumed) rules for remote trusted IT products allowed to connect to the TOE via the network interface) through the SSL enhanced web interface.

During its initialization ("boot up") process, the TOE inspects the checksum of all system software. If any component fails this test, the TOE will halt all initialization functions and require a reboot prior to proceeding with startup. If the problem persists, the TOE will prompt the user or system administrator to place a call to Xerox for a service technician.

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

6.1.12 User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation to support encryption and decryption of designated portions of the hard disk where user files may be stored. Those packages include provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-192-FIPS-197.

6.2 Rationale for TOE Summary Specification

This section demonstrates that the TSFs and Assurance Measures meet the SFRs and SARs.

The specified TSFs work together to satisfy the TOE SFRs. Table 20 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 20: Mapping of SFRs to Security Functions

TSF	SFR	Rational
TSF_IOW	FDP_RIP.1 (IOW 1) FDP_RIP.1 (IOW 2)	TSF_IOW implements FDP_RIP.1 by ensuring that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing.
	FDP_IFF.1 (IOW) FDP_IFC.1 (IOW)	TSF_IOW implements FDP_IFF.1 (IOW) and FDP_IFC.1 (1) by ensuring that all temporary document image data of abnormally terminated jobs will be overwritten once the TOE is turned back on after a power failure. Additionally, the TSF ensures that the complete space reserved for temporary document image data can be overwritten “on demand” by the system administrator.
	FMT_MSA.3 (IOW) FMT_MSA.1 (IOW)	The types of possible jobs are statically defined within the TOE and cannot be modified.
TSF_FLOW	FDP_IFC.1 (FLOW) FDP_IFF.1 (FLOW)	TSF_FLOW implements FDP_IFC.1 (FLOW) and FDP_IFF.1 (FLOW) because it implements the secure store-and-forward principle in both directions based on the rules defined in TSP_FLOW.
	FMT_MSA.3 (FLOW) FMT_MSA.1 (FLOW)	The possible command types and the address spaces of the copy controller and the FAX board are statically defined within the TOE. Nobody is

TSF	SFR	Rational
		able to modify these parameters.
TSF_SYS_AUT	FIA_UAU.2	TSF_SYS_AUT ensures that system administrators must authenticate before accessing the security functionality of the TOE.
	FIA_UID.2	TSF_SYS_AUT ensures that the system administrators must be identified (to include the implicit identification when the “Tools” menu is entered at the Local User Interface) before accessing the security functionality of the TOE.
	FIA_UAU.7	TSF_SYS_AUT ensures that only obscured feedback is generated by the authentication process.
	FIA_AFL.1 (AUT 1)	TSF_SYS_AUT ensures that the TOE locks the Local User Interface until the power is cycled if three unsuccessful authentication attempts happened at this user interface.
	FIA_AFL.1 (AUT 2)	TSF_SYS_AUT ensures that the TOE provides an error message at the Web User Interface to a particular Browser session, if one unsuccessful authentication attempt happened from this Browser session.
	FMT_SMR.1	TSF_SYS_AUT only knows the role “system administrator”.
TSF_NET_AUT	FIA_UID.2	TSF_NET_AUT ensures that users must be identified before being permitted to use TOE network resources.
	FIA_UAU.2	TSF_NET_AUT ensures that users must authenticate (via third party methods such as Kerberos or LDAP) before accessing the network resources of the TOE.
	FAU_GEN.1	TSF_NET_AUT uses the authenticated user name as part of the job context in the system audit log.
TSF_FAU	FAU_GEN.1	TSF_FAU ensures that the TOE generates audit logs of system and user actions/events.
	FAU_SAR.1	TSF_FAU ensures that the system administrator has the capability to review the audit logs.
	FAU_SAR.2	TSF_FAU ensures that the capability of reviewing the audit logs is restricted to the system administrator.

TSF	SFR	Rational
	FAU_STG.1	TSF_FAU ensures that the audit logs cannot be deleted or modified.
	FAU_STG.4	TSF_FAU ensures that the audit log will not fill up so that events are not recorded.
	FPT_STM.1	TSF_FAU ensures that the TOE will have access to a reliable timestamp for marking audit records.
	FIA_UID.2 FIA_UAU.2	TSF_FAU ensures that user identities can be associated with their actions as recorded in the audit logs.
TSF_FCS	FCS_CKM.1 (SSL 1) FCS_CKM.1 (SSL 2)	TSF_FCS ensures that the TOE generates cryptographic keys as defined in the SSL v3 standard with key sizes of 128-bit (RC4), 56-bit (DES) and 168-bit (Triple DES) that meet the generation and exchange of session keys a defined in the SSL v3 standard with the cipher suites defined in FCS_COP.1 (SSL 2). TSF_FCS ensures that the TOE generates cryptographic keys in accordance with OpenSSL RSA key pair generation with key sizes of 1024 bits. TSF_FCS ensures that the TOE generates cryptographic keys in accordance with Triple Data Encryption Standard (3DES-EDE) with key sizes of 3 unique 56-bit keys that meet FIPS-42-2, FIPS-74, FIPS-81.
	FCS_CKM.1 (IPSEC)	TSF_FCS ensures that the TOE generates cryptographic keys as defined in the NIST 800-67 standard for 3DES.
	FCS_CKM.1 (SNMP)	TSF_FCS ensures that the TOE generates cryptographic keys in accordance with DES as specified in the SNMPv3 standard.
	FCS_CKM.1 (UDE)	TSF_FCS ensures that the TOE generates 192-bit AES cryptographic keys.
	FCS_CKM.2 (SSL 1) FCS_CKM.2 (SSL 2)	TSF_FCS ensures that the TOE distributes cryptographic keys in accordance with RSA encrypted exchange of session keys for SSL handshake that meets the SSLv3 standard. TSF_FCS ensures that the TOE distributes cryptographic keys in accordance with digital certificates for public RSA keys that meets the certificate format given in X.509v3.

TSF	SFR	Rational
	FCS_CKM.4	TSF_FCS ensures that the TOE destroys cryptographic keys in accordance with semiconductor memory state loss at power-down, semiconductor memory zeroization at power-up.
	FCS_COP.1 (SSL 1) FCS_COP.1 (SSL 2) FCS_COP.1 (SSL 3)	TSF_FCS ensures that the TOE performs digital signature generation and verification in accordance with AES (256 bits) and RSA (1024 bits) that meets the SSLv3 standard. TSF_FCS ensures that the TOE performs encryption and decryption in accordance with RC4 (128 bit), DES (56 bit) and Triple DES (168-bit) that meet SSLv3 standard – SSL RSA WITH RC4 128 SHA cipher suite. TSF_FCS ensures that the TOE performs digital signature verification in accordance with RSA 1024-bit or smaller keys as specified in the SSLv3 standard.
	FCS_COP.1 (IPSEC 1) FCS_COP.1 (IPSEC 2)	TSF_FCS ensures that the TOE performs IPSec Security Association data encryption and decryption as well as ESP bulk data encryption and decryption as specified in NIST 800-67 standard for 3DES. TSF_FCS ensures that the TOE performs cryptographic checksum generation and secure hash (message digest) computation in accordance with MD5 that meets RFC1321. TSF_FCS also ensures that the TOE performs cryptographic checksum generation and hashing computation in accordance with the SHA-1 algorithm as specified in FIPS 180-2.
	FCS_COP.1 (SNMP 1)	TSF_FCS ensures that the TOE performs hashing and verification in accordance with HMAC – SHA-1 as specified in the SNMPv3 standard.
	FCS_COP.1 (SNMP 2)	TSF_FCS ensures that the TOE performs encryption and decryption in accordance with DES as specified in the SNMPv3 standard.
	FCS_COP.1 (UDE)	TSF_FCS ensures that the TOE encrypts user data on the hard drive using 192-bit AES keys.
TSF_FDP_SSL	FCS_CKM.1 (SSL 1)	TSF_FDP_SSL ensures that the TOE generates cryptographic keys as defined in the SSL v3 standard with key sizes of 128-bit (RC4), 56-bit (DES), or 168-bit (3DES) that meet the

TSF	SFR	Rational
		generation and exchange of session keys a defined in the SSL v3 standard with the cipher suites defined in FCS_COP.1 (SSL 2).
	FCS_CKM.1 (SSL 2)	TSF_FDP_SSL ensures that the TOE generates cryptographic keys in accordance with OpenSSL RSA key pair generation with key sizes of 1024 bits.
	FCS_CKM.2 (SSL 1)	TSF_FDP_SSL ensures that the TOE distributes cryptographic keys in accordance with RSA encrypted exchange of session keys for SSL handshake that meets the SSLv3 standard.
	FCS_CKM.2 (SSL 2)	TSF_FDP_SSL ensures that the TOE distributes cryptographic keys in accordance with digital certificates for public RSA keys that meets the certificate format given in X.509v3.
	FCS_COP.1 (SSL 1)	TSF_FDP_SSL ensures that the TOE performs digital signature generation and verification in accordance with RSA (1024 bits) that meets the SSLv3 standard.
	FCS_COP.1 (SSL 2)	TSF_FDP_SSL ensures that the TOE performs encryption and decryption in accordance with RC4, DES or 3DES that meet the SSLv3 standard.
	FDP_IFC.1 (SSL)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP on Web clients; all web-based traffic to/from that destination; HTTP commands.
	FDP_IFF.1 (SSL)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP based on web clients and servers – X.509 certificates and based on web clients user roles. TSF_FDP_SSL ensures that the TOE permits an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: SSL session establishment and maintenance are in accordance with the SSLv3 standard; the SSL cryptographic operations are in accordance with the SSLv3 standard as implemented within the OpenSSL cryptographic libraries; the signature on any(all) X.509 certificate received by the MFD is valid; all web-based traffic to and from the remote IT entity shall be over an HTTPS connection.

TSF	SFR	Rational
	FDP_UCT.1 (SSL)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.
	FDP_UIT.1 (SSL)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion, and/or replay and to be able to determine on receipt of user data, whether modification, deletion, insertion, and/or replay has occurred.
	FMT_MSA.3 (SSL) FMT_MSA.1 (SSL)	The SSL parameters are statically defined within the TOE and cannot be modified.
	FTP_ITC.1	TSF_FDP_SSL ensures that the TSF provides a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. TSF_FDP_SSL ensures that the TOE permits the TSF to initiate communication via the trusted channel and that the TSF initiates communication via the trusted channel for transmission of network scan data to the scan repository.
	FTP_TRP.1 (SSL)	TSF_FDP_SSL ensures that the TSF provides a communication channel between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
TSF_FDP_FILTER	FDP_IFC.1 (FILTER)	TSF_FDP_FILTER ensures that the TOE enforces the IPFilter SFP on external entities that send traffic to the TOE; all TCP or UDP-based traffic to/from that destination; operations that pass network traffic.
	FDP_IFF.1 (FILTER)	TSF_FDP_FILTER ensures that the TOE enforces the IPFilter SFP based on source IP address. TSF_FDP_FILTER ensures that the TOE permits an information flow between a controlled subject and controlled information via a controlled

TSF	SFR	Rational
		operation if the following rules hold: the source IP address is in the TOE's rule base. TSF_FDP_FILTER ensures that the TOE enforces the implicit allow if no rule is found, explicitly authorizes an information flow if the rule is the default all, and explicitly denies an information flow if there are no rules with matching security attributes.
	FMT_MSA.3 (FILTER) FMT_MSA.1 (FILTER)	The IPFilter parameters (source address) can be defined by the system administrator.
TSF_FDP_IPSEC	FCS_CKM.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TOE generates 3DES cryptographic keys for IPSec.
	FCS_COP.1 (IPSEC 1)	TSF_FDP_IPSEC ensures that the TOE performs correct IPSec Security Association encryption/decryption and ESP bulk data encryption/decryption.
	FCS_COP.1 (IPSEC 2)	TSF_FDP_IPSEC ensures that the TOE generates checksums and hashes in accordance with SHA-1.
	FDP_IFC.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TOE enforces the IPSec SFP on clients; all IP-based traffic to/from that destination.
	FDP_IFF.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TOE enforces the IPSec SFP based on IP-based traffic to and from the remote IT entity shall be over an IPSec connection.
	FDP_UCT.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TOE enforces the IPSec SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.
	FDP_UIT.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TOE enforces the IPSec SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion, and/or replay and to be able to determine on receipt of user data, whether modification, deletion, insertion, and/or replay has occurred.
	FDP_TRP.1 (IPSEC)	TSF_FDP_IPSEC ensures that the TSF provides a communication channel between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or

TSF	SFR	Rational
		disclosure.
	FMT_MSA.3 (IPSEC) FMT_MSA.1 (IPSEC)	The IPSEC parameters are statically defined within the TOE and cannot be modified.
TSF_NET_MGMT	FCS_CKM.1 (SNMP)	TSF_NET_MGMT ensures that the TOE generates DES cryptographic keys for SNMP.
	FCS_COP.1 (SNMP 1)	TSF_NET_MGMT ensures that the TOE performs HMAC – SHA-1 hashing and verification.
	FCS_COP.1 (SNMP 2)	TSF_NET_MGMT ensures that the TOE performs DES encryption and decryption.
	FDP_IFC.1 (SNMP)	TSF_NET_MGMT ensures that the TOE enforces the SNMPSec SFP on SNMP managers; all SNMP traffic to/from that SNMP manager; SNMP commands, packages and traps.
	FDP_IFF.1 (SNMP)	TSF_NET_MGMT ensures that the TOE enforces the SNMPSec SFP on SNMP managers; all SNMP traffic to/from that SNMP manager; SNMP commands, packages and traps.
	FDP_UCT.1 (SNMP)	TSF_NET_MGMT ensures that the TOE enforces the SNMPSec SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.
	FDP_UIT.1 (SNMP)	TSF_NET_MGMT ensures that the TOE enforces the SNMPSec SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion, and/or replay and to be able to determine on receipt of user data, whether modification, deletion, insertion, and/or replay has occurred.
	FMT_MSA.3 (SNMP) FMT_MSA.1 (SNMP)	The SNMP parameters are statically defined within the TOE and cannot be modified.
	FTP_TRP.1 (SNMP)	TSF_NET_MGMT ensures that the TSF provides a communication channel between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
TSF_FMT	FDP_ACC.1 FDP_ACF.1	TSF_FMT ensures that the TOE will restrict access to management interfaces and objects to the system administrator.

TSF	SFR	Rational
	FMT_SMF.1	TSF_FMT provides the security management functions enable/disable IIO and ODIO, change system administrator PIN, and invoke/abort ODIO
	FMT_MOF.1 (FMT 1) FMT_MOF.1 (FMT 2)	TSF_FMT restricts the access to these management functions to the system administrator.
	FMT_SMR.1	TSF_FMT ensures that the TOE maintains a security administrator role and can associate a human user with that role.
	FMT_MTD.1 (AUT) FMT_MTD.1 (SNMP) FMT_MTD.1 (FILTER)	TSF_FMT ensures that the ability to modify certain TSF data is restricted to the system administrator.
	FPT_TST.1	TSF_FMT ensures that the TSF is working properly by providing TOE self testing during initial start-up.
TSF_EXP_UDE	FCS_CKM.1 (UDE)	TSF_EXP_UDE ensures that the TOE generates 192-bit AES keys for disk encryption.
	FCS_COP.1 (UDE)	TSF_ESP_UDE ensures that the TOE encrypts and decrypts data on the hard drive with 192-bit AES cryptographic keys.

7 Definitions

7.1 Terms

In the CC, many terms are defined in Section 3 of Part 1. The following terms are a subset of those definitions:

Authentication data Information used to verify the claimed identity of a user.

Authorized User A user who may, in accordance with the TOE Security Policy (TSP[5]), perform an operation.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Human user Any person who interacts with the TOE.

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.

Object An entity within the TOE Security Function (TSF[6]) Scope of Control (TSC[7]) that contains or receives information and upon which subjects perform operations.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Subject An entity within the TSC that causes operations to be performed.

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

The following terminology is specific to this ST.

FAX A generic reference to one of the Fax types supported by the Device.

[5] TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.
As defined in the CC, Part 1, version 2.3:

[6] TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

[7] TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

Image Data Information on a mass storage device created by the copy (landscape/stapled type only)/print/scan/e-mail process.

Latent Image Data Residual information remaining on a mass storage device when a copy (landscape/stapled type only)/print/scan/ e-mail job is completed, cancelled, or interrupted.

Security Functional Components Express security requirements intended to counter threats in the assumed operating environment of the TOE.

System Administrator An authorized user who manages the Xerox Corporation WorkCentre/WorkCentre Pro.

7.2 Acronyms

The following acronyms are used in this Security Target:

AFL	Authentication Failures
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CPSR	Copy/Print, Store and Reprint
EAL	Evaluation Assurance Level
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High Level Design
IIO	Immediate Image Overwrite
IOS	Image Overwrite Security
IOT	Image Output Terminal
ISO	International Standards Organization
IT	Information Technology
LUI	Local User Interface
MFD	Multi-function Device
MOF	Management of Functions
ODIO	On Demand Image Overwrite
OSP	Organization Security Policy
PP	Protection Profile
PPM	Pages Per Minute
PSTN	Public Switched Telephone Network
RIP	Residual Information Protection
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SM	Security Management
SMF	Security Management Functions
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication (
UI	User Interface
UID	User Identification
WebUI	Web User Interface