Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target

Version 1.0

Prepared by:

Xerox Corporation
1350 Jefferson Road
Rochester, New York 14623

Computer Sciences Corporation
7231 Parkway Drive
Hanover, MD 21076

This page intentionally left blank.

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 and 5, Security Objectives 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), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets Evaluation Assurance Level (EAL) 2.

ST Title:	Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target
ST Version:	1.0
Revision Number:	Revision 1.20
Publication Date:	May 24, 2007
Authors:	Computer Sciences Corporation, Common Criteria Testing Laboratory
TOE Identification:	Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (also known as ISO 15408)
ST Evaluator:	Computer Sciences Corporation (CSC)
Keywords:	Xerox, Multi Function Device, Image Overwrite, WorkCentre, WorkCentre Pro

1.2 References

The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3, CCIMB-2005-08-001

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3, CCIMB-2005-08-002

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3, CCIMB-2005-08-003

[CEM] Common Evaluation Methodology for Information Technology Security Evaluation, dated August 2005, Version 2.3, CCIMB-2005-08-004

1.3 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

The CC allows several operations to be performed on security functional components; *assignment, refinement*, *selection,* and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

a) The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

b) The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

d) *Iterated* functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1 (1) and FMT_MTD.1 (2).

e) Plain *italicized text* is used to emphasize text.

1.3.2 Terminology

In the CC, many terms are defined in Section 2.3 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[1]), 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[2]) Scope of Control (TSC[3]) 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.

Security Functional Components Express security requirements intended to counter threats in the assumed operating environment of 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 (i.e., embedded analog fax (fax board), I-FAX (see below), LanFax (see below), and Server Fax (not part of the evaluation).

Image Data Information on a mass storage device created by the print, scan, e-mail, I-FAX, or LanFax processes.

LanFax A TOE function in which the data is sent to the device as a print job, but rather than being output as a hardcopy, it is sent out through the embedded analog fax board (optional).

Latent Image Data Residual information remaining on a mass storage device when a print, scan, e-mail, I-FAX, or LanFax job is completed, cancelled, or interrupted.

System Administrator An authorized user who manages the TOE.

[1] 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 2.1:
[2] 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.
[3] TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

1.3.3 Acronyms

The following acronyms are used in this Security Target:

ACRONYM	DEFINITION
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DES	Data Encryption Standard
DH	Diffie-Hellman
DMA	Direct Memory Access
EAL	Evaluation Assurance Level
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of Security Functions
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High Level Design
IIO	Immediate Image Overwrite
ISO	International Standards Organization
IPSec	Internet Protocol Security
ISO 15408	Common Criteria 2.2 ISO Standard
IT	Information Technology
MFD	Multifunction Device
MOF	Management of Functions
MTD	Management of TSF Data
ODIO	On-Demand Image Overwrite
OSP	Organization Security Policy
PP	Protection Profile
PSTN	Publicly Switched Telephone Network
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Scanner Image Processor
SM	Security Management
SMR	Security Management Roles
SMTP	Simple Mail Transfer Protocol
SNMPv3	Simple Network Management Protocol, Version 3
SOF	Strength of Function
SSL	Secure Socket Layer

ACRONYM	DEFINITION
SSLv2	Secure Socket Layer, Version 2
SSLv3	Secure Socket Layer, Version 3
ST	Security Target
TDES	Triple DES
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection
UI	User Interface

1.4 TOE Overview

The TOE is a multi-function device (MFD) with the Image Overwrite Security accessory, the embedded fax accessory, and in the WorkCentre Pro models, the Network Scanning accessory, all consumer options. The Overwrite Security accessory causes any temporary image files created during a print, network scan, scan-to-email, and LanFax job to be overwritten when those files are no longer needed or “on demand” by the system administrator. Copy and embedded fax jobs do not get written to the HDD. The Network Scanning option utilizes the inherent TOE SSL support to secure the filing of scanned documents on a remote SSL-enabled server.

User image files associated with the Store Print and Scan-to-Mailbox feature may be stored long term for later reprinting. Files are stored in an encrypted partition of the hard disk. These files are overwritten automatically when deleted by the user, or when “on demand” image overwrite is executed by the system administrator.

The Xerox Embedded Fax accessory provides local analog fax capability over PSTN connections and also enables LanFax jobs.

The TOE also provides support for other network security protocols, such as IPSec and SNMPv3, to protect user data. Additionally, the TOE can be configured to filter inbound network traffic based on the provided address, port. Finally, the TOE also maintains an audit log.

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

1.5 Common Criteria Conformance Claim

This ST conforms to CC Part 2 extended and is CC Part 3 augmented (with ALC_FLR.3) at the EAL 2 level of assurance.

2 TOE DESCRIPTION

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The TOE is a multi-function device (MFD) that copies and prints, with scan to e-mail, network scan, and FAX options. The TOE includes the Image Overwrite Security accessory. This accessory forces any temporary image files created during a print, network scan, scan to email, or LanFax job to be overwritten when those files are no longer needed. An additional package (optional in the evaluation) is the network scanning package

Table 1: Models and capabilities

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

	Print	Copy[1]	Network Scan	Embedded Fax[1]	Scan 2 email
WorkCentre 232	x	x	n/a	o	x
WorkCentre 238	x	x	n/a	o	x
WorkCentre 245	x	x	n/a	o	x
WorkCentre 255	x	x	n/a	o	x
WorkCentre 265	x	x	n/a	o	x
WorkCentre 275	x	x	n/a	o	x
WorkCentre Pro 232	x	x	x	o	x
WorkCentre Pro 238	x	x	x	o	x
WorkCentre Pro 245	x	x	x	o	x
WorkCentre Pro 255	x	x	x	o	x
WorkCentre Pro 265	x	x	x	o	x
WorkCentre Pro 275	x	x	x	o	x

[1] Copy and embedded FAX jobs are not spooled to the HDD.

The MFD stores temporary image data created during a print, network scan or scan to email, and LanFAX job on an internal hard disk drive (HDD). This temporary image data consists of the original data submitted and additional (scratch) files scan created during a job. Copy and local FAX jobs do not get written to the HDD.

In the base evaluated configuration, the TOE, with the Image Overwrite Security accessory, provides an image overwrite function to enhance the security of the MFD. This function overwrites temporary document image data as described in DoD Standard 5200.28-M either at the completion of each print, network scan, scan to email, or LanFAX job, or *on demand* of the MFD system administrator. A system administrator may use the *on demand* image overwrite security option to clear sensitive information from the HDD when the MFD is, for example, decommissioned.

User image files associated with the Store Print and Scan-to-Mailbox feature may be stored long term for later reprinting. Files are stored in an encrypted partition of the hard disk. The encryption key is created dynamically on each power-up. 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 on-demand image overwrite.

Note: The overwrite patterns used for stored jobs are the same patterns specified by 5200.28-M; however, since the patterns are written through the encryption algorithm, they get written to the disk as randomized data. Therefore, the overwrite algorithm used for the encrypted partition is not technically in compliance with 5200.28-M.

The TOE configuration, with respect to the WorkCentre Pro models, adds Xerox's Network Scanning Accessory. This accessory allows documents to be scanned at the device with the resulting image being stored on a remote server/repository. The connection between the device and the remote server is secured when the TOE's SSL support is enabled; the transfer of the data is through an HTTPS connection.

All models of the TOE have the optional Embedded FAX accessory is added. This accessory permits the TOE to function as a local Fax connected to the PSTN.

All models of the TOE support both auditing and 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 secure network scan data transfer); system administrator download of the device's audit log; IPSec support for lpr and port 9100 print jobs; secure network device management through SNMPv3, and specification of IP filtering rules.

Figure 1: Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275

*** Also shown are an optional paper feeder and finisher.**

2.2 Physical Scope and Boundary

The TOE is a Multi-Function Device, shown in Figure 1, which performs printer, copier, scanner, LanFax, embedded analog FAX (optional), and email functions.

The physical scope and boundary of the TOE consists of the Xerox WorkCentre or WorkCentre Pro devices and include installed Xerox accessories. For this evaluation, all models of the TOE will include the Image Overwrite Security accessory and the embedded FAX accessory. The configuration options found on the "Special Purpose Pages" of the WebUI (see http://www.xerox.com/security) are not a part of the evaluated configuration. In the WorkCentre Pro models the Network Scanning accessory (a software component) is included in the configuration.

Table 2: Evaluated Software/Firmware version

Software/Firmware Item	WorkCentre	WorkCentre + PostScript	WorkCentre Pro
System Software	**12.060.17.000**	**14.060.17.00**	**13.060.17.000**
Network Controller Software	**040.022.00115**	**040.022.10115**	**040.022.50115**
UI Software	**012.60.012**	**012.60.012**	**012.60.012**
IOT Software	**50.04.00**	**50.04.00**	**50.04.00**
SIP Software	**12.60.05**	**12.60.05**	**12.60.05**
DADH Software (Options)			
• Normal Mode	**14.00.00**	**14.00.00**	**14.00.00**
• Quiet Mode	**15.12.00**	**15.12.00**	**15.12.00**
FAX Software	**02.28.013**	**02.28.013**	**02.28.013**
Finisher Software (Options)			
• 1K LCSS	**01.27.00**	**01.27.00**	**01.27.00**
• 2K LCSS	**03.20.00**	**03.20.00**	**03.20.00**
• HCSS	**13.38.00**	**13.38.00**	**13.38.00**
• HCSS with BookletMaker	**24.10.00**	**24.10.00**	**24.10.00**
Scanner Software (Options)			
• 232/238/245/255 PPM[1] Models	**17.05.00**	**17.05.00**	**17.05.00**
• 265/275 PPM[1] Models	**04.09.00**	**04.09.00**	**04.09.00**

The TOE physical boundary also consists of the Administrative and User Guidance provided on CDs with the device, as well as, the Secure Operation guidance provided to consumers through the Xerox web site (www.xerox.com).

2.3 Logical Scope and Boundary

The TOE logical boundary composed of two distinct security approaches: the architecture of the TOE, and the security functions provided by the TOE.

Architecturally, the TSF cannot be bypassed, corrupted, or otherwise compromised. Whereas the TOE is an MFD and not a general purpose computer, there are no untrusted subjects, or processes, contained therein, and the TSF functions in its own domain (Security Architecture – TSF_ARCH). While not a TSF in the classic sense of the term, the functionality that would be associated with TSF_ARCH is present and represented by the security functional requirements (SFRs) FPT_RVM.1 and FPT_SEP.1 based strictly on the TOE definition and architecture.

The following security functions are controlled by the TOE:

- Image Overwrite (TSF_IOW)
- System Authentication (TSF_SYS_AUT)
- Network Identification (TSF_NET_ID)
- 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)
- FAX Flow Security (TSF_FAX_FLOW)
- Security Management (TSF_FMT)
- User Data Protection - AES (TSF_EXP_UDE)

2.3.1 Image Overwrite (TSF_IOW)

The TOE implements an image overwrite security function, through the Image Overwrite Security accessory, to overwrite temporary files created during the printing, network scan, scan-to-email, and LanFax processes. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. Copy and local FAX jobs do not get written to the HDD. Once the job has completed, the files are automatically overwritten using a three pass overwrite procedure as described in DOD 5200.28-M (Immediate Image Overwrite (IIO) and "On-Demand" Image Overwrite (ODIO)). The overwrite patterns used for stored jobs are the same patterns specified by 5200.28-M; however, since the patterns are written through the encryption algorithm, they get written to the disk as randomized data. The TSF_IOW function, ODIO, can also be invoked manually by the system administrator. A scheduling function allows ODIO to be executed on recurring basis as set up by the System Administrator.

The ODIO is invoked by the System Administrator via the tools menu/web interface. Once invoked, the ODIO cancels all jobs, halts the network interface, and overwrites the contents of the reserved section on the hard disk (it utilizes the same three-pass procedure identified above), and then the network controller reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

2.3.2 System Authentication (TSF_SYS_AUT)

The TOE utilizes a simple authentication function through the front panel or web interface. The system administrator must authenticate by entering a 3 to 12 digit PIN prior to being granted access to the tools menu and system administration functions (**NOTE**: Xerox security guidance documentation specifies the use of a PIN between 8 and 12 digits). The system administrator must change the default PIN after installation is complete. While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered.

The Web user interface also requires the system administrator to enter a PIN and enter "admin" into the username field. Additional users cannot be added. The TOE does not associate privileged-user attributes or privileges based on username.

2.3.3 Network Identification (TSF_NET_ID)

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 (Solaris), Kerberos (Windows 2000), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000).

2.3.4 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, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit records; the downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

2.3.5 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, SNMPv3.

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

2.3.6 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 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. If the system administrator-managed function is enabled, then the TOE creates and enforces the informal security policy model, “All communications to the Web server will utilize SSL (HTTPS).”

2.3.7 User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is generated by the system administrator specifying a series of rules to “accept,” “deny,” or “drop” packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

2.3.8 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.

2.3.9 Network Management Security (TSF_NET_MGMT)

The TOE supports SNMPv3 as part of its security solution (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.

2.3.10 FAX Flow Security (TSF_FAX_FLOW)

The TOE is architected to provide separation between the optional FAX processing board and the network controller.

The FAX card plugs directly into the PCI bus of the SIP (Scanner Image Processor) board with the SIP acting as the PCI bus master. The SIP communicates with the network controller via the industry standard FireWire interface, but it is the SIP/FAX interface that provides TSF_FAX_FLOW.

There are two methods of communication between the SIP and the FAX – Command/Response and Image data transfer. Commands and Responses are sent and received via a shared memory block on the FAX card. Image data is transferred using DMA transfer with the SIP acting as the bus master. For outgoing fax the SIP will push image data to the FAX card. For incoming fax the SIP will pull image data from the FAX. The FAX card will inform the SIP when there is a FAX available for collection. Similarly, the SIP will inform the FAX card when it wishes to send a fax out.

2.3.11 Security Management (TSF_FMT)

The TOE restricts access to the configuration of administrative functions to the system administrator by implementing the PrivUserAccess SFP. Under this SFP, the TOE utilizes the front panel software module security mechanisms to allow only the authenticated system administrator the capability to:

- Enable or disable the TSF_IOW function;
- Change the system administrator PIN;
- Abort ODIO;
- Manually invoke “On Demand” Image Overwrite.

The SFP also controls the Web UI connected over a secure connection (https) to allow only the system administrator, the PrivUserAccess SFP, to manage the following security functions:

- Manually invoke “On Demand” image overwrite;
- Establish a recurrence schedule for “On Demand” image overwrite;
- Enable/disable SSL support;
- Enable/disable and configure IPSec tunneling;
- Enable/disable and configure SNMPv3;
- Create/install X.509 certificates;
- Enable/disable and download the audit log;
- Enable/disable and configure (rules) IP filtering.

As indicated in Section 2.3.6 above SSL must be enabled and configured before the system administrator can utilize the secure Web UI to manage IPSec and SNMPv3, and to download the audit log.

2.3.12 User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, 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-128-FIPS-197.

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

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage 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.

3.1.1 Environment Assumptions

The environmental assumptions delineated in Table 3 are required to ensure the security of the TOE:

Table 3: Environmental Assumptions

Assumption	Description
Physical	
A.INSTALL	The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.PHYSICAL_PROTECT	The TOE will be located within facilities providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE and the TOE serial port.
Personnel	
A.MANAGE	There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the system administration documentation.
A.PROCEDURE	Procedures exist for granting system administrator(s) access to the TSF.
A.CHANGE_SA_PIN	System administrators PIN is changed according to the following: 8-digit PIN every 40 days 9-digit PIN every year

Assumption	Description
Connectivity	
A.SANE_NETWORK	All network components connected to the network to which the TOE is connected pass data correctly without willful or malicious 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, SSH, IPSec, SNMPv3) and work as advertised.

3.2 Threats

3.2.1 Threats Addressed by the TOE

Table 4 identifies the threats addressed by the TOE. These threats are considered to be users with public knowledge of how the TOE operates. However, the threats do not possess access to the resources necessary to recover latent residual information from a HDD. The threats have access to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 4: Threats Addressed by the TOE

Threat	Description
T.RECOVER	A malicious user may attempt to recover temporary document image data from a print/network scan/email/LanFax job by removing the HDD and using commercially available tools to read its contents. This scenario may occur as part the life-cycle of the MFD (e.g., decommission) or as a more overt action.
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.FAXLINE	A malicious user may attempt to access the internal network (to access data and/or resources) via the FAX telephone line/modem using publicly available tools and equipment (the threat agent does not have access to specialized digital/analog telephone/modem/computer/etc. equipment).

3.2.2 Threats Addressed by the IT Environment

Table 5 below specifies and describes the threat against which protection from the IT environment is required.

Table 5: Threat 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 6 below enumerates the organizational security policies the TOE must comply with:

Table 6: Organizational Security Policy(s)

Policy	Description

P.COMMS_SEC	TOE supported network security mechanisms (i.e., HTTPS, IPSec ESP and/or AH, SNMPv3, 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).
P.SSL_ENABLED	Secure Socket layer network security mechanisms shall be supported by the TOE and enabled.

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 7.

Table 7: 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.RESIDUAL	Temporary document image data, from an MFD function that utilizes the HDD for storage, must not remain on the hard disk drive once that job is completed.
O.MANAGE	The TOE will provide the functions and facilities necessary to support system administrators responsible for the management of the TOE and must allow only system administrators access to this functionality.
O.RESTRICT	The TOE will prevent access to the network from the telephone line via the TOE's FAX modem.
O.ONDEMAND	The TOE will provide the system administrator with the ability to invoke the image overwrite function "on demand."
O.CONTROL_ACCESS	The TOE will provide the system administrator with the ability to determine network access/information flow to the TOE for trusted remote IT products.
O.PROTECTCOM	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.
O.PROTECTDAT	The TOE must protect user data stored for the purpose of reprinting in the future from disclosure, or modification.

4.2 Security Objectives for the Environment

The security objectives for the non-IT Environment are defined in Table 8.

Table 8: Security Objectives for the Non-IT Environment

Objectives	Description
OE.MANAGE	A responsible individual will be assigned as the system administrator who will see that the TOE is installed and operated in accordance with all applicable policies and procedures necessary to operate the TOE in a secure manner.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are effectively protected against physical attack within the facility.

The security objectives for the IT Environment are defined in Table 8a.

Table 9a: Security Objectives for the IT Environment

Objectives	Description
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.
OE.PROTECT_COM	The TOE environment must protect user data from disclosure, or modification, by establishing a trusted channel between itself and the TOE when SSL is enabled over which the data is transported prior to data transmission.

5 IT 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 TOE Security Functional Requirements

The TOE satisfies the SFRs delineated in Table 10. The rest of this section contains a description of each component and any related dependencies.

Table 10: 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_COP.1	Cryptographic operation
FCS_CKM.4	Cryptographic key destruction
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

Functional Component ID	Functional Component Name
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FMT_MOF.1	Management of security functions behavior
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamp
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted Path

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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

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

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

c. [assignment: none].

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

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

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: the events specified in Table 11 below].

Table 11: Audit Events

The audit log will have the following fixed size entries:

- Entry number (an integer value from 1 to the number of entries in the audit log)
- Event Date (mm/dd/yy)
- Event Time (hh:mm:ss)
- Event ID (a unique integer value – see table entries below)
- Event Description (a brief description of an entry that should match the unique Entry ID value – see table entries below)
- Entry Data (This value is any additional data that is logged for an audit log entry – see table entries below)

Event ID	Event Description	Entry Data Contents
1	System startup	Device name; Device serial number
2	System shutdown	Device name; Device serial number
3	ODIO started	Device name; Device serial number
4	ODIO complete	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	LAN Fax job NOTE: this entry is for Network (Server) Fax which is not part of this evaluation and is only provided for completeness.	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.
8	IFAX	Job name; User Name; Completion Status; IIO status; Accounting User ID; Accounting Account ID; total-number-of smtp-recipients; smtp-recipients
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	Print/Fax Driver NOTE: this entry corresponds to LanFax	Job name; User Name; Completion Status; IIO status; Accounting User ID; Accounting Account ID; total-fax-recipient-phone-numbers; fax-recipient-phone-numbers.

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.

Dependencies: FPT_STM.1 Reliable time stamp

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

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.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit Review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: None.

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

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to:	FAU_STG.3.
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.
Dependencies:	FAU_STG.1 Protected audit trail storage

5.1.2 Class FCS: Cryptographic Support

SSL Specific

FCS_CKM.1 (1) Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1(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 [128-bit (RC4)] 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 (2)].
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

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.

FCS_CKM.1 (2) Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1(2)	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [OpenSSL RSA key pair generation] and specified cryptographic key sizes [1024 bits] that meet the following: [not specified].
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

Application note: The SSL v3 standard does not define how the RSA key pair is generated; the definition is implementation dependent – in this case based on the OpenSSL cryptographic libraries. 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.

FCS_CKM.2 (1) Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1(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].

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
FMT_MSA.2 Secure security attributes

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

FCS_CKM.2 (2) Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1(2) 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].

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

FMT_MSA.2 Secure security attributes

FCS_COP.1 (1) **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1(1) The TSF shall perform [digital signature generation and verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [1024 bits] that meet the following: [SSLv3 standard].

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
FMT_MSA.2 Secure security attributes

FCS_COP.1 (2) **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1(2) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [RC4] and cryptographic key sizes [128 bit] that meet the following: [SSLv3 standard – SSL_RSA_WITH_RC4_128_SHA cipher suite].

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
FMT_MSA.2 Secure security attributes

IPSec Specific

FCS_CKM.1(3) **Cryptographic key generation**

Hierarchical to: No other components.

FCS_CKM.1.1(3) 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: [FIPS-42-2, FIPS-74, FIPS-81].

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_COP.1(3) Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1(3)(1) The TSF shall perform [

a) IPSec Security Association data encryption/decryption specified by IKE in RFC2409 as defined in the TOE security policy; and

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

in accordance with a specified cryptographic algorithm [3DES-EDE] and cryptographic key sizes [168 bits] that meet the following: [FIPS-42-2, FIPS-74, FIPS-81].

FCS_COP.1.1(3)(2) The TSF shall perform [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [N/A] that meet the following: [RFC1321].

FCS_COP.1.1(3)(3) The TSF shall perform [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [N/A] that meet the following: [FIPS-186].

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
FMT_MSA.2 Secure security attributes

SNMPv3 Specific

FCS_CKM.1 (4) **Cryptographic key generation**

Hierarchical to: No other components.

FCS_CKM.1.1(4) 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 (4)].

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_COP.1 (4) **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1(4) 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].

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
FMT_MSA.2 Secure security attributes

Disk Encryption Specific

FCS_CKM.1 (5) **Cryptographic key generation**

Hierarchical to: No other components.

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [128 bit] that meet the following: [Xerox proprietary string upon boot up].

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_COP.1 (5) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(5) The TSF shall perform [encryptions and decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bit] that meet the following: [none].

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
FMT_MSA.2 Secure security attributes

End of Security Mechanism specific Cryptographic Security Functional Requirements

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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].

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]
FMT_MSA.2 Secure security attributes

5.1.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

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

- Subjects: authorized users;
- Information: management interfaces;
- Operations: access management interfaces].

Dependencies: FDP_ACF.1 Simple security attributes

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

- Subjects: Authorized users – role;
- Objects: Management interfaces – 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 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].

Dependencies: FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static attribute initialisation

FDP_IFC.1(1) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(1) The TSF shall enforce the [IPFilter SFP] on [

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

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(1) **Simple security attributes**

Hierarchical to: No other components.

FDP_IFF.1.1(1) The TSF shall enforce the [IPFilter SFP] based on the following types of subject and information security attributes: [

- Subjects: Source IP address, destination TCP or UDP port,
- Information: none].

FDP_IFF.1.2(1) 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 is in the TOE's rule base
- If configured, the destination transport layer port is in the TOE's rule base.]

FDP_IFF.1.3(1) The TSF shall enforce the [implicit allow if no rule is found].

FDP_IFF.1.4(1) The TSF shall provide the following [none].

FDP_IFF.1.5(1) The TSF shall explicitly authorize an information flow based on the following rules: [if the rule is the default all].

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization.

FDP_IFC.1(2) **Subset information flow control**

Hierarchical to: No other components.

FDP_IFC.1.1(2) The TSF shall enforce the [IPSec SFP] on [

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

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(2) **Simple security attributes**

Hierarchical to: No other components.

FDP_IFF.1.1(2) The TSF shall enforce the [IPSec SFP] based on the following types of subject and information security attributes: [

- Subjects: Printing clients – presumed address;
- Information: none].

FDP_IFF.1.2(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 IP-based traffic to and from the client destination passes through the IPSec tunnel until either end powers down, or resets (after which the tunnel must be reestablished)
- IPSec tunnel mode for communication with a particular destination presumes the address of the printing client]

FDP_IFF.1.3(2) The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4(2) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5(2) The TSF shall explicitly authorize an information flow based o the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.6(2) The TSF shall explicitly deny any information flow based on the following rules: [not additional rules based on security attributes that explicitly deny information flows].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFC.1(3) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(3) The TSF shall enforce the [SSLSec SFP] on [

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

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(3) **Simple security attributes**

Hierarchical to: No other components.

FDP_IFF.1.1(3) The TSF shall enforce the [SSLSec SFP] based on the following types of subject and information security attributes: [

- Subjects: web clients and servers – X.509 certificates; web clients – user role;
- Information: none].

FDP_IFF.1.2(3) 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 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]

FDP_IFF.1.3(3) The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4(3) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5(3) The TSF shall explicitly authorize an information flow based o the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.6(3) The TSF shall explicitly deny any information flow based on the following rules: [not additional rules based on security attributes that explicitly deny information flows].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFC.1(4) **Subset information flow control**

Hierarchical to: No other components.

FDP_IFC.1.1(4) The TSF shall enforce the [SNMPSec SFP] on [

- Subjects: SNMP managers;
- Information: All SNMP traffic to/from that destination;

- Operations: SNMP commands, SNMP traps].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(4) **Simple security attributes**

Hierarchical to: No other components.

FDP_IFF.1.1(4) The TSF shall enforce the [SNMPSec SFP] based on the following types of subject and information security attributes: [

- Subjects: SNMP managers – authentication data in SNMP message;
- Information: SNMP message time value].

FDP_IFF.1.2(4) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- SNMP managers request SNMP management information, or issue SNMP commands from the MFD/agent.
- The agent verifies the authentication code
- The agent verifies the timeliness of the SNMP message
- The agent successfully decrypts the SNMP "message"
- All SNMP-based traffic to and from the client destination passes through the MFD's/agent's SNMP security subsystem (as defined in the SNMPv3 specification]

FDP_IFF.1.3(4) The TSF shall enforce the [no additional information flow control SFP rules].

FDP_IFF.1.4(4) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5(4) The TSF shall explicitly authorize an information flow based o the following rules: [no additional rules based on security attributes that explicitly authorize information flows].

FDP_IFF.1.6(4) The TSF shall explicitly deny any information flow based on the following rules: [not additional rules based on security attributes that explicitly deny information flows].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_RIP.1 **Subset Residual Information Protection**

Hierarchical to: No other components

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [Hard Disk Drive].

Dependencies: No dependencies

FDP_UCT.1(1) Basic data exchange confidentiality

Hierarchical to: No other components

FDP_UCT.1.1(1) The TSF shall enforce the [IPSec SFP] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

Dependencies: [FDP_ITC.1 Inter-TSF Trusted channel

FTP_TRP.1 Trusted Path]

[FDP_ACC.1 Subset Access Control or

FDP_IFC.1 Subset information flow control]

FDP_UIT.1(1) Data exchange integrity

Hierarchical to: No other components

FDP_UIT.1.1(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*.

FDP_UIT.1.2(1) The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.

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_UCT.1(2) Basic data exchange confidentiality

Hierarchical to: No other components

FDP_UCT.1.1(2) The TSF shall enforce the [SSLSec SFP] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel

FTP_TRP.1 Trusted Path]

[FDP_ACC.1 Subset Access Control or

FDP_IFC.1 Subset information flow control]

FDP_UIT.1(2) **Data exchange integrity**

Hierarchical to: No other components

FDP_UIT.1.1(2) 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*.

FDP_UIT.1.2(2) The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.

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_UCT.1(3) **Basic data exchange confidentiality**

Hierarchical to: No other components

FDP_UCT.1.1(3) The TSF shall enforce the [SNMPSec SFP] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel

FTP_TRP.1 Trusted Path]

[FDP_ACC.1 Subset Access Control or

FDP_IFC.1 Subset information flow control]

FDP_UIT.1(3) **Data exchange integrity**

Hierarchical to: No other components

FDP_UIT.1.1(3) The TSF shall enforce the [SNMPSec SFP] to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and/or replay*.

FDP_UIT.1.2(3) The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.

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]

5.1.4 Class FIA: Identification and Authentication

FIA_AFL.1 **Authentication failure handling**

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [authentication of the System Administrator at the LUI].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [At the local UI, lockout the SA login for a period of 3 minutes].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 **User identification before any action**

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FIA_UAU.2 **User Authentication Before Any Action**

Hierarchical to: FIA_UAU.1 Timing of Authentication

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

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.7 **Protected Authentication Feedback**

Hierarchical to: No other components

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

Dependencies: FIA_UAU.1 Timing of Authentication

5.1.5 Class FMT: Security Management

FMT_MOF.1 **Management of Security Functions Behavior**

Hierarchical to: No other components

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

- TSF_IOW
- TSF_NET_ID
- TSF_FAU
- TSF_FDP_SSL
- TSF_FDP_FILTER
- TSF_FDP_IPSec
- TSF_NET_MGMT]

to [the system administrator].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles

FMT_MTD.1(1) **Management of TSF data**

Hierarchical to: No other components

FMT_MTD.1.1(1) The TSF shall restrict the ability to *clear*, *delete*, [*create*, *read (download)*] the [

- Audit log]

to [the system administrator].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles

FMT_MTD.1(2) **Management of TSF data**

Hierarchical to: No other components

FMT_MTD.1.1(2) The TSF shall restrict the ability to *delete*, [*create*] the [

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

to [the system administrator].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles

FMT_MTD.1(3) Management of TSF data

Hierarchical to: No other components

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query*, *modify*, *delete*, [*creat*e] the [

- IP filter rules]

to [the system administrator].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

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

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [system administrator].
FMT_SMR.1.2	The TSF shall be able to associate **human** users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.1.6 Class FPT: Protection of the TSF

FPT_RVM.1	**Non-bypassability of the TSP**
Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No Dependencies

FPT_SEP.1	**Domain separation**
Hierarchical to:	No other components.
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No Dependencies

FPT_STM.1	**Reliable time stamp**
Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies:	No Dependencies

5.1.7 Class FTP: Trusted path/channels

FTP_ITC.1	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other

communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [transmission of network scan data to the scan repository].

Dependencies: No dependencies

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

Hierarchical to: No other components.

FTP_TRP.1.1(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(1) The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3(1) The TSF shall require use of the trusted path for [

- *Print jobs submitted via lpr or port 9100*].

Dependencies: No dependencies

FTP_TRP.1(2) Trusted path (NOTE: SSLSec SFP)

Hierarchical to: No other components.

FTP_TRP.1.1(2) 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(2) The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3(2) 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*].

Dependencies: No dependencies

FTP_TRP.1(3) **Trusted path (NOTE: SNMPSec SFP)**

Hierarchical to: No other components.

FTP_TRP.1.1(3) 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(3a) The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.2(3b) The TSF shall permit *the TSF* to initiate communication via the trusted path.

FTP_TRP.1.3(3) The TSF shall require use of the trusted path for [*SNMP messages*].

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

Table 12 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2 and includes the augmented SAR, ALC_FLR.3. The SARs are not iterated or refined from Part 3.

Table 12: EAL2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC_FLR.3	Systematic Flaw Remediation	None
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1 AGD_ADM.1, AGD_USR.1

5.3 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

EXP_FAX.1 Network FAX Separation

Hierarchical to:	No other components
EXP_FAX.1.1	Access to the internal network through the FAX telephone line/modem interface shall be denied.
Dependencies:	No dependencies

EXP_UDE.1 User Data Encryption

Hierarchical to:	No other components
EXP_UDE.1.1	The TOE shall encrypt user data stored in a separate partition for the purpose of reprinting at a later time.
Dependencies:	FCS_CKM.1 Cryptographic key generation] FCS_COP.1 Cryptographic operation]

5.5 SFRs With SOF Declarations

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

FIA_UAU.2: The authentication mechanism has a PIN space of 12^3 – 12^{12} (3 – 12 digit PIN). **IMPORTANT NOTE:** through Xerox security guidance the recommended PIN size is 8 to 12 digits (PIN Space of 12^8 to 12^{12}).

EXP_UDE.1: The key used when encrypting user data is generated dynamically upon power up. The key is generated by hashing a Xerox proprietary string . The hash algorithm is SHA-1.

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 5.1.1. Traceability to SFRs is also provided.

- Image Overwrite (TSF_IOW)
- System Authentication (TSF_SYS_AUT)
- Network Identification (TSF_NET_ID)
- 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)
- FAX Flow Security (TSF_FAX_FLOW)
- Security Management (TSF_FMT)
- User Data Protection - AES (TSF_EXP_UDE)

The TOE meets the security functional requirements of FPT_RVM.1 and FPT_SEP.1 based on its architecture and function (which could be expressed as TOE Security Function - Security Architecture or TSF_ARCH). The TSF cannot be bypassed, corrupted, or otherwise compromised. The TOE is an MFD, not a general purpose computer, and as such there are no untrusted subjects or processes contained therein, and the TSF functions in its own domain. The processing paradigm for the TOE is that each “session” on the device is unique and the security functionality cannot be bypassed. Additionally, user interaction with the TOE is such that the transfer of objects between the TOE and the environment are controlled by the TSF such that there can be: no transfer between domains by the user; no uploading of executable code, configuration files, etc. by a non-privileged user; nor can data in the trusted domain be viewed, modified, etc.

6.1.1 Image Overwrite (TSF_IOW)

The TOE implements an image overwrite security function to overwrite temporary files created during the printing, network scan, or scan to email, and LanFax process. The network controller spools and processes documents to be printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. Once the job has completed, the files are overwritten using a three pass overwrite procedure as described in DOD 5200.28-M

(Immediate Image Overwrite (IIO) and "On-Demand" Image Overwrite (ODIO)). The overwrite patterns used for stored jobs are the same patterns specified by 5200.28-M; however, since the patterns are written through the encryption algorithm, they get written to the disk as randomized data. The TSF_IOW function can also be invoked manually by the system administrator (ODIO). A scheduling function allows ODIO to be executed on recurring basis as set up by the System Administrator.

The ODIO is invoked by the System Administrator via the tools menu/web interface. 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, and then the network controller reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

While ODIO is running, the GUI will display a message stating that ODIO is in progress and an abort button. If the System Administrator cancels ODIO, the process stops at a sector boundary. As part of the cancellation, the file system is rebuilt (e.g., the directory is cleared and the i-nodes are initialized and the system then reboots). During every reboot, the system goes through a file system check that verifies the integrity of the directory, and the partitions are remounted as logical partitions.

If the network controller crashes for any reason, it will re-boot. The progress of all jobs is tracked in a log in the network controller. During the re-boot process, the log is tracked and will overwrite all abnormally terminated jobs.

Functional Requirements Satisfied: FDP_RIP.1

6.1.2 System Authentication (TSF_SYS_AUT)

The TOE utilizes a simple authentication function through the front panel or web interface. The system administrator must authenticate by entering a 3-12 digit PIN (NOTE: this is the PIN size inherent to the device, however, Xerox Security guidance specifies the use of a PIN with a minimum of 8 digits) prior to being granted access to the tools menu and system administration functions. The system administrator must change the default PIN after installation is complete. While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered. The authentication mechanism has a PIN space of 12^3 to 12^{12}.

The Web user interface also requires the user to enter a PIN and enter "admin" into the username field. The username prompt provided by the web server is not used. The only valid string is "admin", which is hard coded into the web server and cannot be changed. Additional users cannot be added. The TOE does not associate user attributes or security-based privileges based on username.

The TOE also supports authentication failure handling at the LUI. The number of failed system authentication attempts at the LUI is hard-coded at 3 and cannot be changed.

Functional Requirements Satisfied: FIA_AFL.1, FIA_UID.2, FIA_UAU.2, FIA_UAU.7 FMT_SMR.1

6.1.3 Network Identication (TSF_NET_ID)

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 (Solaris), Kerberos (Windows 2000), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000).

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 6.1.4, Security Audit). The TOE defines one user authentication method: Network Authentication.

Functional Requirements Satisfied: FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FAU_GEN.1

6.1.4 Security Audit (TSF_FAU)

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

The audit log tracks system start-up/shutdown, ODIO start/completion, and print, scan, email, local fax, I-Fax (not evaluated), and LanFax jobs. Copy jobs are not tracked. 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 6.1.3 above). *Network Authentication* is mutually exclusive with *Auditron* and *XSA*, however, it can be enabled concurrently with *Network Accounting*.

The *Auditron* method utilizes a PIN-based identification system that is maintained in a database resident on the copy controller board. The *XSA* method is also PIN-based, however its database is resident on the network 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, email, and IFax (not included in the evaluation) jobs the accounting IDs (i.e., PINS) required by the *Auditron*, *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.

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.

Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FPT_STM.1, FIA_UID.2, FIA_UAU.2, FIA_UAU.7, FIA_AFL.1

6.1.5 Cryptographic Support (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, SNMPv3.

Functional Requirements Satisfied: FCS_CKM.1(1-4), FCS_CKM.2(1-2), FCS_CKM.4, FCS_COP.1(1-4)

6.1.6 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.

Functional Requirements Satisfied: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FSC_CKM.2(2), FCS_COP.1(1), FDP_IFC.1(3), FDP_IFF.1(3), FDP_UCT.1(2), FDP_UIT.1(2) , FTP_ITC.1, FTP_TRP.1(2)

6.1.7 User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is defined by the system administrator through specifying a series of rules to "accept," "deny," or "drop" packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

Functional Requirements Satisfied: FDP_IFC.1(1), FDP_IFF.1(1)

6.1.8 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. 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.

Functional Requirements Satisfied: FCS_CKM.1(3), FCS_CKM.4, FCS_COP.1(3), FDP_IFC.1(2), FDP_IFF.1(2), FDP_UCT.1(1) , FDP_UIT.1(1) , FTP_TRP.1(1)

6.1.9 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 and single-DES in Cipher Block Chaining mode for encryption. SNMPv3 utilizes the OpenSSL crypto library for the authentication and encryption functions.

Functional Requirements Satisfied: FCS_CKM.1(4), FCS_CKM.4, FCS_COP.1(4), FDP_IFC.1(4), FDP_IFF.1(4), FDP_UCT.1(3), FDP_UIT.1(3), FTP_ITC.1, FTP_TRP.1(3)

6.1.10 Information Flow (TSF_FAX_FLOW)

The architecture of the TOE is such that it provides separation between the optional FAX processing board and the network controller.

The FAX card plugs directly into the PCI bus of the SIP board with the SIP acting as the PCI bus master. The SIP communicates with the network controller via the industry standard FireWire interface, but it is the SIP/FAX interface that provides TSF_FLOW

There are two methods of communication between the SIP and the FAX - Command/Response and Image data transfer. Commands and Responses are sent and received via a shared memory block on the FAX card. Image data is transferred using DMA transfer with the SIP acting as the bus master. For outgoing fax the SIP will push image data to the FAX card. For incoming fax the SIP will pull image data from the FAX. The FAX card will inform the SIP when there is a FAX available for collection. Similarly, the SIP will inform the FAX card when it wishes to send a fax out.

No mechanism exists to transfer arbitrary (e.g. non-FAX) data between the SIP and FAX card.

Functional Requirements Satisfied: EXP_FAX.1

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, abort ODIO, 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; establish a recurrence schedule for “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; create/upload/download X.509 certificates; enable/disable and configure IPSec tunneling; enable/disable and configure SNMPv3, and enable/disable and configure (specify the IP address and/or IP address range (presumed), port and port range, for remote trusted IT products allowed to connect to the TOE via the network interface) IP filtering] through the SSL enhanced web interface.

Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_MOF.1, FMT_SMF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3).

6.1.12 User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, 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-128-FIPS-197.

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

Functional Requirements Satisfied: EXP_UDE.1, FCS_CKM.1(5), FCS_COP.1(5)

6.2 Assurance Measures

The TOE satisfies CC EAL2 assurance requirements, augmented with ALC_FLR.3. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Xerox to satisfy the CC EAL2 assurance requirements.

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration Items	The vendor provided configuration management documents and a Configuration Item list.
ADO_DEL.1 Delivery Procedures	The vendor provided delivery procedures.
ADO_IGS.1 Installation, Generation and Startup procedures	The vendor provided secure installation, generation and start up procedures.
ADV_FSP.1 Informal function specification	The vendor provided an informal function specification.
ADV_HLD.1 Descriptive high-level design	The vendor provided a descriptive high-level design document.
ADV_RCR.1 Informal correspondence demonstration	The informal correspondence demonstration is provided in the design documentation. ST to FSP in the FSP, FSP to HLD in the HLD.
AGD_ADM.1 Administrator Guidance	The vendor submitted a system administration manual.
AGD_USR.1 User Guidance	The vendor submitted a user guide.
ALC_FLR.3 Systematic flaw remediation	The vendor submitted instructions and procedures for the reporting, configuration management, and remediation of identified security flaws.
ATE_COV.1 Evidence of coverage	The analysis of test coverage was submitted in the evaluation evidence.
ATE_FUN.1 Functional testing	The test evidence was submitted to the CCTL.
ATE_IND.2 Independent testing – sample	The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.
AVA_SOF.1 Strength of Function	The vendor submitted an analysis of the SOF for the PIN.

Assurance Component	How requirement will be met
AVA_VLA.1 Independent vulnerability analysis	The vendor submitted vulnerability analysis was confirmed. The laboratory conducted an independent vulnerability assessment by building on the vendor's. The laboratory conducted penetration testing.

7 PROTECTION PROFILE (PP) CLAIMS

The TOE does not claim conformance to a PP.

8 RATIONALE

This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability	The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following: • security objectives to threats encountered • environmental objectives to assumptions met • SFRs to objectives met
Assurance Level	A justification is provided for selecting an EAL2 level of assurance for this ST.
SOF	A rationale is provided for the SOF level chosen for this ST.
Dependencies	A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

Table 13: Security Objectives Rationale

Objective	Threat Organizational Security Policy Assumption	Rationale
O.AUDITS	P.HIPAA_OPT	O.AUDITS helps satisfy OSP P.HIPAA_OPT by ensuring that log entries are periodically reviewed 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.
O.RESIDUAL	T.RECOVER	O.RESIDUAL helps to counter the threat T.RECOVER by limiting the amount of time

		that temporary document image data is on the hard disk drive. By removing this temporary data, the window of opportunity is reduced to the time necessary to process the job. The TSF_IOW function overwrites any residual data as described in DoD 5200.28-M.
O.MANAGE	T.RECOVER	The O.MANAGE objective helps to counter the threat T.RECOVER by ensuring that the TOE is properly configured and operating in accordance with stated security guidance.
O.RESTRICT	T.FAXLINE	O.RESTRICT counters the threat T.FAXLINE because it ensures that it is not possible to access the network from the telephone line via the TOE's FAX modem.
O.ONDEMAND	T.RECOVER	O.ONDEMAND helps counter the threat T.RECOVER because by manually invoking the image overwrite function, the system administrator is able to minimize the opportunity an adversary has to access temporary document image data on the HDD from a print, scan to email or network scanning job. O.ONDEMAND also helps counter the threat T.RECOVER when the device is decommissioned or moved. By manually invoking the image overwrite function, the system administrator is able to sanitize the spool partition of the HDD before the device is taken out of service or transported to an insecure site.
O.CONTROL_ACCESS	T.COMM_SEC	O.CONTROL_ACCESS helps mitigate the threat T.COMM_SEC by ensuring that the administrator has the ability to control network access and information flow to prevent an attacker from intercepting communications between the TOE and a remote trusted IT product.
O.PROTECTCOM	T.COMM_SEC P.COMMS_SEC P.SSL_ENABLED	O.PROTECTCOM helps mitigate the threat T.COMM_SEC and 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.
O.PROTECTDAT	T.RECOVER	O.PROTECTDAT helps counter the threat T.RECOVER because it ensures that user data stored on the hard disk is not recoverable when the disk is removed from the system.

Table 14: Security Objectives Rationale for the Environment

Objective	Threat Organizational Security Policy Assumption	Rationale
OE.MANAGE	A.INSTALL A.MANAGE A.NO_EVIL_ADM A.PROCEDURE A.CHANGE_SA_PIN A.SANE_NETWORK	OE.MANAGE is met by A.CHANGE_SA_PIN, A.INSTALL, A.MANAGE, A.PROCEDURE, and A.NO_EVIL_ADM by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE. The OE.MANAGE objective extends to support the assumption that all components connected to the network to which the TOE is connected pass data correctly without modification (A.SANE_NETWORK).
OE.PHYSICAL	A.PHYSICAL_ PROTECT	OE.PHYSICAL is met by the A.PHYSICAL_ PROTECT environmental assumption. This assumption acknowledges the need for the TOE to be located within facilities providing controlled access to prevent unauthorized physical access to critical internal parts of the TOE and the TOE serial port.
OE.NETWORK_I&A	TE.COMM_SEC A.SAME_CONTROL	OE.NETWORK_I&A helps mitigate the threat TE.COMM_SEC and 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 and to ensure that such remote products are under the same management and subject to the same security policy as the TOE.
OE.PROTECT_COM	TE.COMM_SEC P.COMMS_SEC P.SSL_ENABLED A.EXT_RFC_COMPLIANT	OE.PROTECT_COM helps mitigate the threat TE.COMM_SEC and meet the OSPs P.COMMS_SEC AND P.SSL_ENABLED by ensuring that a trusted communication channel between the TOE and remote trusted IT

Objective	Threat Organizational Security Policy Assumption	Rationale
		products is established to protect user data from disclosure or modification. A.EXT_RFC_COMPLIANT 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.

8.2 Security Requirements Rationale

This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Rationale for TOE Security Requirements

This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following paragraphs provide the security requirement to security objective mapping and a rationale to justify the mapping.

Table 15: Rationale for TOE Security Requirements

SFR	Rationale
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. This SFR traces back to and aids in meeting the following objectives: O.MANAGE and O.AUDITS
FAU_SAR.1 FAU_SAR.2	Ensures 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. This SFR traces back to and aids in meeting the following objectives: O.MANAGE and O.AUDITS
FAU_STG.1 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. These SFRs trace back to and aid in meeting the following objective: O.AUDITS

SFR	Rationale
FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1	Ensure that the TOE provides the cryptographic support and services 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. These SFRs trace back to and aids in meeting the following objectives: O.CONTROL_ACCESS and O.PROTECTCOM. Ensure that the TOE provides the cryptographic support and services and associated key management capabilities necessary to assure data protection for stored files by using specified cryptographic key generation algorithms and associated cryptographic key distribution and destruction methods. These SFRs trace back to and aids in meeting the following objectives: O.CONTROL_ACCESS and O.PROTECTDAT.
FDP_ACC.1 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. These SFRs trace back to and aid in meeting the following objectives: O.CONTROL_ACCESS, O.PROTECTCOM
FDP_IFC.1 FDP_IFF.1 FDP_RIP.1 FDP_UCT.1 FDP_UIT.1	Ensure that the IP_Filter SFP and IP Security SFP are enforced to control and protect information flow between controlled subjects (IP address, destination port, etc.) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner and the protection and removal of residual user data from a controlled resource. These SFRs trace back to and aids in meeting the following objectives: O.RESIDUAL, O.CONTROL_ACCESS, O.PROTECTCOM
FIA_AFL.1	Ensures that the TOE takes specific and immediate action when the set threshold of unsuccessful login attempts by the System Administrator is reached. This SFR traces back to and aids in meeting the following objective(s): O.MANAGE
FIA_UID.2 FIA_UAU.2 FIA_UAU.7	Ensures that the System Administrator and other users are successfully identified and securely (obscured feedback only) authenticated before being allowed to perform any activity managed by the TOE. These SFRs trace back to and aids in meeting the following objective(s): O.MANAGE

SFR	Rationale
FMT_MOF.1	Ensures that only system administrators have the capability to enable, disable, or manually invoke specific, security-relevant capabilities of the TOE. This SFR traces back and aids in meeting the following objective: O.MANAGE.
FMT_MTD.1	Ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to query, modify, delete, create, or install specified security attributes, keys and certificates, and IP filter rules. This SFR traces back to and aids in meeting the following objective(s): O.MANAGE, O.CONTROL_ACCESS, O.PROTECTCOMM, O.AUDITS
FMT_SMF.1	Ensures that critical security management functions (i.e., enable/disable IIO, change system administrator PIN, invoke/abort ODIO, enable/disable or configure cryptographic applications, etc.) are available on the TOE. This SFR traces back and aides in meeting the following objectives: O.MANAGE, O.ONDEMAND, O.PROTECTCOM.
FMT_SMR.1	Ensures that the TOE maintains the system administrator role – a trusted individual who can administer the TOE. This SFR traces back and aids in meeting O.MANAGE and O.ONDEMAND.
FPT_RVM.1	Ensures that TOE security policy enforcement functions are invoked and successful before any TOE function is allowed to proceed. This SFR traces back to and aids in meeting the following objective(s): O.MANAGE, O.PROTECTCOM
FPT_SEP.1	Ensures that the TOE maintains a security domain for its own use to protect against interference or tampering by untrusted subjects and provides a reliable time stamp for information flow control decisions and audit event logging. This SFR traces back to and aid in meeting the following objective(s): O.CONTROL_ACCESS
FPT_STM.1	Ensures that the TOE provides a reliable timestamp for inclusion in the audit log. This SFR traces back to and aids in meeting the following objective: O.AUDITS
FTP_ITC.1 FTP_TRP.1	Ensures 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. This SFR traces back to and aids in meeting the following objective: O.MANAGE, O.PROTECTCOM

SFR	Rationale
EXP_FAX.1	Network FAX separation protects TSF and its data from modification or tampering. O.RESTRICT is met by the architectural design of the TOE to make it impossible for an external entity to access TSF data or the network through the telephone line/modem of the optional FAX.
EXP_UDE.1	Data encryption protects the confidentiality and integrity of user data files that are stored on the TOE's hard disk for the purpose of reprinting at a later time. This SFR traces back to and aids in meeting the following objective: O.PROTECTDAT,

Table 16: TOE SFR Mapping to Objectives

	O.AUDITS	O.RESIDUAL	O.MANAGE	O.RESTRICT	O.ONDEMAND	O.CONTROL_ACCESS	O.PROTECT.COM	O.PROTECTDAT
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						X	X	X
FCS_CKM.2						X	X	X
FCS_CKM.4						X	X	X
FCS_COP.1						X	X	X
FDP_ACC.1						X	X	
FDP_ACF.1						X	X	
FDP_IFC.1		X				X	X	
FDP_IFF.1		X				X	X	
FDP_RIP.1		X				X	X	
FDP_UCT.1		X				X	X	
FDP_UIT.1		X				X	X	

FIA_AFL.1			X					
FIA_UID.2			X					
FIA_UAU.2			X					
FIA_UAU.7			X					
FMT_MOF.1			X					
FMT_MTD.1	X		X			X	X	
FMT_SMF.1			X		X		X	
FMT_SMR.1			X		X			
FPT_RVM.1			X				X	
FPT_SEP.1						X		
FPT_STM.1	X							
FTP_ITC.1			X				X	
FTP_TRP.1			X				X	
EXP_FAX.1				X				
EXP_UDE.1								X

8.3 Rationale For Assurance Level

This ST has been developed for multi-function digital image processing products incorporating an Image Overwrite Security accessory. The TOE environment will be exposed to a low level of risk because the TOE sits in office space where it is under almost constant supervision. Agents cannot physically access the HDD or FAX without disassembling the TOE. Agents have no means of infiltrating the TOE with code to effect a change. As such, the Evaluation Assurance Level 2 is appropriate. That Assurance Level is augmented with ALC_FLR.3, Systematic Flaw Remediation procedures. That requirement ensures that instructions and procedures for the reporting, configuration management, and remediation of identified security flaws are in place.

8.4 Rationale For TOE Summary Specification

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

The specified TSFs work together to satisfy the TOE SFRs. Table 17 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 17: Mapping of SFRs to Security Functions

SFR	Name	TSF	Name
FAU_GEN.1	Audit data generation	TSF_NET_ID TSF_FAU	Network Identification Security Audit
FAU_SAR.1	Audit review	TSF_FAU	Security Audit
FAU_SAR.2	Restricted audit review	TSF_FAU	Security Audit

SFR	Name	TSF	Name
FAU_STG.1	Protected audit trail storage	TSF_FAU	Security Audit
FAU_STG.4	Prevention of audit data loss	TSF_FAU	Security Audit
FCS_CKM.1	Cryptographic key generation	TSF_FCS TSF_FDP_SSL TSF_NET_MGMT TSF_FDP_IPSec TSF_EXP_UDE	Cryptographic Support User Data Protection – SSL Network Management Security User Data Protection – IPSec User Data Protection - AES
FCS_CKM.2	Cryptographic key distribution	TSF_FCS TSF_FDP_SSL	Cryptographic Support User Data Protection - SSL
FCS_CKM.4	Cryptographic key destruction	TSF_FCS TSF_FDP_IPSec TSF_NET_MGMT	Cryptographic Support User Data Protection – IPSec User Data Protection - SNMP
FCS_COP.1	Cryptographic operation	TSF_FCS TSF_FDP_SSL TSF_FDP_IPSec TSF_NET_MGMT TSF_EXP_UDE	Cryptographic Support User Data Protection – SSL User Data Protection – IPSec Network Management Security User Data Protection - AES
FDP_ACC.1	Subset access control	TSF_FMT	Security Management
FDP_ACF.1	Access control functions	TSF_FMT	Security Management
FDP_IFC.1	Subset information flow control	TSF_FDP_SSL TSF_FDP_FILTER TSF_FDP_IPSec TSF_NET_MGMT	User Data Protection – SSL User Data Protection – IP Filtering

SFR	Name	TSF	Name
			User Data Protection – IPSec Network Management Security
FDP_IFF.1	Simple security attributes	TSF_FDP_SSL TSF_FDP_FILTER TSF_FDP_IPSec TSF_NET_MGMT	User Data Protection – SSL User Data Protection – IP Filtering User Data Protection – IPSec Network Management Security
FDP_RIP.1	Subset residual information protection	TSF_IOW	Image Overwrite
FDP_UCT.1	Basic data exchange confidentiality	TSF_FDP_SSL TSF_FDP_IPSec TSF_NET_MGMT	User Data Protection – SSL User Data Protection – IPSec Network Management Security
FDP_UIT.1	Data exchange integrity	TSF_FDP_SSL TSF_FDP_IPSec TSF_NET_MGMT	User Data Protection – SSL User Data Protection – IPSec Network Management Security
FIA_AFL.1	Authentication failure handling	TSF_SYS_AUT TSF_FAU	System Authentication Security Audit
FIA_UID.2	User identification before any action	TSF_SYS_AUT TSF_NET_ID TSF_FAU	System Authentication Network Identification Security Audit
FIA_UAU.2	User authentication before any action	TSF_SYS_AUT TSF_NET_ID TSF_FAU	System Authentication Network Identification Security Audit

SFR	Name	TSF	Name
FIA_UAU.7	Protected authentication feedback	TSF_SYS_AUT TSF_NET_ID TSF_FAU	System Authentication Network Identification Security Audit
FMT_MOF.1	Management of security functions behavior	TSF_FMT	Security Management
FMT_MTD.1	Management of TSF data	TSF_FMT	Security Management
FMT_SMF.1	Specification of management functions	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_SYS_AUT TSF_FMT	System Authentication Security Management
FPT_RVM.1	Non-bypassability of the TSP	TSF_ARCH	Security Architecture
FPT_SEP.1	TSF domain separation	TSF_ARCH	Security Architecture
FPT_STM.1	Reliable time stamp	TSF_FAU	Security Audit
FTP_ITC.1	Inter-TSF trusted channel	TSF_FDP_SSL TSF_NET_MGMT	User Data Protection – SSL Network Management Security
FTP_TRP.1	Trusted Path	TSF_FDP_SSL TSF_FDP_IPSec TSF_NET_MGMT	User Data Protection – SSL User Data Protection – IPSec Network Management Security
EXP_FAX.1	Network FAX Separation	TSF_FAX_FLOW	Information Flow
EXP_UDE.1	User Data Encryption	TSF_EXP_UDE	User Data Protection - AES

8.4.1 TOE Assurance Requirements

Section 6.2 of this document identifies the Assurance Measures implemented by Xerox to satisfy the assurance requirements of EAL2 as delineated in the table in Annex B of the CC, Part 3. Table 18 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 18: Assurance Measure Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Life Cycle	Test	Vulnerability Assessment
ACM_CAP.2	X						
ADO_DEL.1		X					
ADO_IGS.1		X					
ADV_FSP.1			X				
ADV_HLD.1			X				
ADV_RCR.1			X				
AGD_ADM.1				X			
AGD_USR.1				X			
ALC_FLR.3				X	X		
ATE_COV.1						X	
ATE_FUN.1						X	
ATE_IND.2						X	
AVA_SOF.1							X
AVA_VLA.1							X

8.4.2 TOE SOF Claims

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. The claim of SOF-basic ensures that the Image Overwrite mechanism is resistant to a low attack potential because the residual information cannot be accessed by subjects without sophisticated data recovery tools. Furthermore, the claim SOF-basic ensures that an unskilled attacker cannot access the internal network from the telephone FAX/modem.

8.5 Rationale For SFR and SAR Dependencies

Table 19 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 19: SFR Dependencies Status

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FAU_GEN.1	Audit data generation	FPT_STM.1	Yes
FAU_SAR.1	Audit review	FAU_GEN.1	Yes
FAU_SAR.2	Restricted audit review	FAU_SAR.1	Yes
FAU_STG.1	Protected audit trail storage	FAU_GEN.1	Yes
FAU_STG.4	Prevention of audit data loss	FAU_STG.1	Yes
FCS_CKM.1	Cryptographic key generation	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	Yes Yes No[4]
FCS_CKM.2	Cryptographic key distribution	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Yes Yes No[4]
FCS_CKM.4	Cryptographic key destruction	FDP_ITC.1 or FCS_CKM.1 FMT_MSA.2	Yes No[4]
FCS_COP.1	Cryptographic operation	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	Yes Yes No[4]
FDP_ACC.1	Subset access control	FDP_ACF.1	Yes
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	Yes No[5]
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Yes
FDP_IFF.1	Simple security attributes	FDP_IFC.1 FMT_MSA.3	Yes No[5]

[4] The TOE does not check for key correctness.

[5] The security functional requirement FMT_MSA.3 (Secure security attributes) is not supported by the TOE. SSL does not support the concept of "permissive, restrictive, [other values]" for default security attributes, nor does it support "authorized user role" definition of alternative initial values.

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FDP_RIP.1	Subset residual information protection	None	
FDP_UCT.1	Basic data exchange confidentiality	FDP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	Yes Yes
FDP_UIT.1	Data exchange integrity	FDP_ACC.1 or FDP_IFC.1 FDP_ITC.1 or FTP_TRP.1	Yes Yes
FIA_AFL.1	Authentication failure handling	FIA_UAU.1	Yes
FIA_UID.2	User identification before any action	None	
FIA_UAU.2	User authentication before any action	FIA_UAU.1	Yes
FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	Yes
FMT_MOF.1	Management of security functions behavior	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MTD.1	Management of TSF data	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_SMF.1	Specification of management functions	None	
FMT_SMR.1	Security Roles	FIA_UID.1	Yes
FPT_RVM.1	Non-bypassability of the TSP	None	
FPT_SEP.1	TSF domain separation	None	
FPT_STM.1	Reliable time stamp	None	
FTP_ITC.1	Inter-TSF trusted channel	None	
FTP_TRP.1	Trusted Path	None	
EXP_UDE.1	User Data Encryption	FCS_CKM.1 FCS_COP.1	Yes

SAR dependencies identified in the CC have been met by this ST as shown in Table 20.

Table 20: EAL2 SAR Dependencies Satisfied

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	NA
ADO_DEL.1	Delivery procedures	None	NA
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	YES
ADV_FSP.1	Informal functional specification	ADV_RCR.1	YES
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	YES
ADV_RCR.1	Informal correspondence demonstration	None	YES
AGD_ADM.1	Administrator guidance	ADV_FSP.1	YES
AGD_USR.1	User guidance	ADV_FSP.1	YES
ALC_FLR.3	Systematic Flaw Remediation	None	NA
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	YES
ATE_FUN.1	Functional testing	None	NA
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	YES
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	YES
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	YES

8.6 Rationale for Explicitly Stated Requirements

The CC does not provide a security functional requirement that adequately represents the TOE security functionality associated with the FAX interface/functionality. Any attempt to use the CC permitted security functional requirement operations over multiple CC specified security functional requirements (i.e., FPT_SEP.1, and FDP_IFC.1, and FDP_IFF.1) would, at best, create an incoherent specification – for both implementation and evaluation. For this reason, it was necessary to write an explicitly stated requirement, EXP_FAX.1, that states that the TSF will separate the network and FAX interfaces. This requirement is necessary to provide isolation between the FAX telephone line/modem and the network interface.

The CC does not provide a security functional requirement that adequately represents the TOE security functionality associated with disk encryption. For this reason, it was necessary to write an explicitly stated requirement, EXP_UDE.1, that states that the TSF will encrypt user data files that are stored for the purpose of reprinting at a later time.

8.7 Internal Consistency and Mutually Supportive Rationale

The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Table 17. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 19 and Table 20 and described in Section 8.6.

c) The SARs are appropriate for the assurance level of EAL2 and are satisfied by the TOE as shown in Table 18. EAL2 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.