Xerox WorkCentre 5030/5050 Multifunction Systems

Security Target

Version 1.0

Prepared by:

Xerox Corporation
1350 Jefferson Road
Rochester, New York 14623

Computer Sciences Corporation (US)
7231 Parkway Drive
Hanover, Maryland 21076

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 B, and Part 3, Chapter 10.

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, augmented with ALC_FLR.3.

ST Title:	Xerox WorkCentre 5030/5050 Multifunction Systems Security Target
ST Version:	1.0
Revision Number:	Revision: 1.18
Publication Date:	April 15, 2008
Certification Number:	BSI-DSZ-CC-0478
Authors:	Computer Sciences Corporation (US) Common Criteria Testing Laboratory, Xerox Corporation
Sponsor:	Xerox Corporation
TOE Identification:	Xerox WorkCentre 5030/5050 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

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 or assurance components; *assignment, refinement, selection,* and *iteration* as defined in paragraph 6.4.1.3.2 of Part 1 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 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.
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)).
Image Data	Information on a mass storage device created by the print/scan/e-mail process.
Latent Image Data	Residual information remaining on a mass storage device when a print/scan/ e-mail job is completed, cancelled, or interrupted.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.
System Administrator	An authorized user who manages the Xerox Corporation WorkCentre/WorkCentre Pro.

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 2.3:
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
AFL	Authentication Failures (CC Family)
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
DADH	Duplex Automated Document Handler
EAL	Evaluation Assurance Level
FDP	User Data Protection (CC Class)
FIA	Identification and Authentication (CC Class)
FMT	Security Management (CC Class)
FSP	Functional Specification (CC Family)
HDD	Hard Disk Drive
HLD	High Level Design (CC Family)
IIO	Immediate Image Overwrite
IOS	Image Overwrite Security
IOT	Image Output Terminal
ISO	International Standards Organization
IT	Information Technology
LUI	Local User Interface
MFD	Multi-function Device
MOF	Management of Functions (CC Family)
ODIO	On Demand Image Overwrite
OSP	Organization Security Policy
PP	Protection Profile
PPM	Pages Per Minute
PSTN	Public Switched Telephone Network
RIP	Residual Information Protection (CC Family)
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Scanner Image Processor
SM	Security Management
SMF	Ssecurity Management Functions (CC Family)
SMR	Security Management Roles (CC Family)
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

ACRONYM	DEFINITION
UAU	User Authentication (CC Family)
UI	User Interface
UID	User Identification (CC Family)
WebUI	Web User Interface

1.4 TOE Overview

The TOE is a multi-function device (MFD) that provides copy and print services as well as the scan to e-mail, network scan and FAX options. A standard component of the TOE is the Image Overwrite Security package. This function forces any temporary image files created during a print, network scan, or scan to e-mail job to be overwritten when those files are no longer needed, or "on demand" by the system administrator. Because copy and FAX jobs are not written to the hard disk drive (HDD), there are no temporary images files to be overwritten for these services.

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

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 conformant, and is CC Part 3 conformant, EAL2 augmented (with ALC_FLR.3).

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 product is a MFD that copies and prints, with scan to e-mail, network scan and FAX option. A standard component of the TOE is the Image Overwrite Security package. This function forces any temporary image files created during a print, network scan, or scan to e-mail job to be overwritten when those files are no longer needed.

The optional Xerox Embedded Fax accessory, when purchased and installed, provides local analog fax capability over PSTN connections.

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

Table 1: Models and capabilities

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

	Print	Copy[1]	Network Scan	FAX[1]	Scan to e-mail	Print Speed
WorkCentre 5030	X	X	o	o	o	Up to 30ppm
WorkCentre 5050	X	X	o	o	o	Up to 50ppm

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

A MFD stores temporary image data created during a print, network scan or scan to e-mail job on an internal hard disk drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job. Because copy and FAX jobs are not written to the HDD, there are no temporary images files to be overwritten for these services.

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

2.2 Physical Scope and Boundary

The TOE is a Multi-Function Device (Xerox WorkCentre model 5030 or 5050) that consists of a printer, copier, scanner, FAX (when purchased by the consumer), and e-mail as well as all Administrator and User guidance. The difference between the two models is their printing speed. The hardware included in the TOE is shown in Figure 1. This figure also shows an optional Finisher connected to the TOE at the right side of the picture, which is not part of the TOE. The optional FAX card is not shown in this figure.[4]

Figure 1: Xerox WorkCentre 5030/5050

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

The **UI software** controls the User Interface. **SIP software** controls the Copy Controller and is able to interface with all other software components. **IOT software** controls the marking engine that prints to paper. **DADH software** controls the input tray. **Finisher software** controls the optional Finisher attachment. **FAX software** resides on the FAX board and controls some fax functions. The **System software** manages overall system function while the **Network Controller software** resides on the Network Controller and controls all network functions.

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

Table 2: Evaluated Software/Firmware version

Software Item	WorkCentre 5030/5050
System Software	**5. 003.07.000**
Network Controller Software	**1.08.535.01**
UI Software	**005.03.007**
SIP Software	**50.06.00**
IOT Software	**23.54.00**
DADH Software	**12.15.00**
Finisher Software	**09.21.00**
FAX Software	**02.28.03**

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

2.3 Logical Scope and Boundary

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

The following security functions are provided by the TOE:

- Image Overwrite (TSF_IOW)
- Authentication (TSF_AUT)
- Security Management (TSF_FMT)
- Information Flow (TSF_FLOW)

2.3.1 Image Overwrite (TSF_IOW)

The TOE has an "Image Overwrite" function that overwrites files created during print, network scan or scan to e-mail jobs. This overwrite process is implemented in accordance with DoD 5200.28-M and will be activated at the completion of each print, network scan, or scan to e-mail job, once the MFD is turned back on after a power failure or *on demand* of the MFD system administrator. Copy and FAX jobs are not written to the hard drive and need not to be overwritten.

2.3.2 Information Flow (TSF_FLOW)

The TOE does not allow information to flow between the PSTN port of the optional FAX processing board (if installed) and the network controller (which covers the information flow to and from the internal network). Data and/or commands cannot be sent to the internal network via

the PSTN. A direct connection from the internal network to external entities by using the telephone line of the TOE is also denied.

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

2.3.3 Authentication (TSF_AUT)

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

2.3.4 Security Management (TSF_FMT)

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

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

2.4 Evaluated Configuration

In its evaluated configuration, the Image Overwrite Security Package is installed and IIO and ODIO are enabled on the TOE. The FAX option, if purchased by the consumer, is installed and enabled. All other configuration parameter values are optional.

3 TOE SECURITY ENVIRONMENT

3.1 Assumptions

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

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

Table 3: Environmental Assumptions

Assumption	Description
A.INSTALL	The TOE has been delivered and installed by Xerox-authorized representatives using Xerox delivery and installation guidance. The TOE has been configured by the system administrator in accordance with the administrator and user guidance delivered with the TOE as well as the security guidance found at http://www.xerox.com/security. As a part of this installation process, the system administrator has changed the PIN from its default value. The PIN chosen by the administrator consists of at least 8 digits and will be changed at least every 40 days. The Image Overwrite Security accessory is installed and enabled. IIO and ODIO are enabled.
A.ACCESS	The TOE has been installed in a standard office environment. Because the TOE is under observation by office personnel, unauthorized physical modifications to the TOE and unauthorized attempts to connect to the TOE via its physical interfaces are not possible.
A.MANAGE	One or more system administrators are assigned to manage the TOE. Procedures exist for granting a system administrator access to the system administrator PIN for the TOE.
A.NO_EVIL_ADM	The system administrator(s) are not careless, willfully negligent or hostile, and will follow the instructions provided in the administrator and user guidance delivered with the TOE as well as the security guidance found at http://www.xerox.com/security. The system administrator will not remove the TOE from its evaluated configuration and will especially not disable TSF_IOW.
A.NETWORK	The network that the TOE is connected to will be monitored for unapproved activities and/or attempts to attack network resources (including the TOE).

3.2 Threats

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

Table 4: Threats to the TOE

Threat	Description
T.RECOVER	A malicious user may attempt to recover temporary document image data using commercially available tools to read its contents. This may occur because the attacker gets physical access to the hard disk drive (e.g. as part the life-cycle of the MFD (e.g. decommission)), or the temporary document image data can be read/recovered over the network (e.g. as the result of a purposeful or inadvertent power failure before the data could be erased.)
T.INFAX	During times when the FAX is not in use, a malicious user may attempt to access the internal network by connecting to the FAX card via PSTN and using publicly available T.30 FAX transmission protocol commands for the purpose of intercepting or modifying sensitive information or data that may reside on resources connected to the network. This threat only exists if the FAX board is installed and connected to the PSTN.
T.OUTFAX	During times when the FAX is not in use, a malicious user may attempt to connect to the TOE over the network and make an outgoing connection using the FAX card, either as a method of attacking other entities or for the purpose of sending sensitive information or data to other entities.[5] This threat only exists if the FAX board is installed and connected to the PSTN.
T.USER	A user, at any time, may attempt to reconfigure the TOE, for the purpose of disabling security functions or intercepting sensitive information or data, either by attempting to access the management functions directly or by logging in as the system administrator.

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

3.3 Organizational Security Policies

There are no organizational security policies that are determined to be relevant for the TOE.

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 5.

Table 5: Security Objectives for the TOE

Objectives	Description
O.RECOVER	Temporary document image data from a print, network scan or scan to e-mail job must be overwritten on the hard disk drive in accordance with DoD 5200.28-M immediately after that job is completed or once the TOE is turned back on after a power failure. Temporary document image data from these jobs must also be overwritten at the command ("on demand") of the system administrator. Copy and FAX (if installed) jobs must not be written to the hard drive at all.
O.FAXLINE	The TOE will not allow access to the internal network from the telephone line via the TOE's FAX modem (if installed). Likewise, the TOE will not allow accessing the PSTN port of the TOE's FAX modem (if installed) from the internal network.

Objectives	Description
O.MANAGE	The TOE will provide the functions and facilities necessary to support system administrators responsible for the management of the TOE. The TOE must require that system administrator(s) authenticate with a PIN before allowing access to management functions. The PIN must be obscured as it is entered by the system administrator. The Local UI will be locked for 2 minutes once 5 invalid login attempts have been detected when trying to cancel an ODIO operation. The Local UI will be locked for 3 minutes once 3 invalid login attempts have been detected for all other local administrator operations. The WebUI will send an error code after every invalid authentication attempt.

4.2 Security Objectives for the Environment

4.2.1 Security objectives for the IT Environment

Table 6: Security Objectives for the IT Environment

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

4.2.2 Security objectives for the non IT Environment

Table 7: Security Objectives for the non-IT Environment

Objectives	Description
OE.INSTALL	System administrator oversees installation, configuration and operation of the TOE by Xerox-authorized representatives in accordance with the Xerox delivery and installation guidance. The TOE must be configured by the system administrator in accordance with the system administration and user guidance as well as with the security guidance found at http://www.xerox.com/security. As part of the installation process, the system administrator has to change the PIN from its default value to a value with at least 8 digits. The system administrator has to change the PIN at least every 40 days. The system administrator ensures that the TOE will be configured

Objectives	Description
	according to the configuration under evaluation and will not remove the TOE from its evaluated configuration. Especially Image Overwrite Security accessory is installed and enabled and IIO and ODIO are enabled.
OE.ACCESS	The TOE will be located in an office environment where it will be monitored by the office personnel for unauthorized physical connections, manipulation or interference.
OE.ADMIN	At least one responsible and trustworthy individual (system administrator) will be assigned, according to onsite procedures for granting access to the PIN, to manage the TOE. The individual(s) have to follow the instructions provided in the administrator and user guidance as well as the security guidance found at http://www.xerox.com/security

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 Security Policies

This chapter contains the definition of security policies which must be followed by the TOE and implemented by the TSF.

5.1.1 User Data Protection Policy (TSP_IOW)

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

- Temporary document image data from a print, network scan or scan to e-mail job must be overwritten on the hard disk drive in accordance with DoD 5200.28-M immediately after that job is completed.

- All temporary document image data of abnormally terminated jobs must be overwritten in accordance with DoD 5200.28-M once the MFD is turned back on after a power failure.

- The space on the hard disk drive reserved for temporary document image data must be overwritten in accordance with DoD 5200.28-M, if the system administrator has invoked the On Demand Image Overwrite function.

- Document image data of copy and FAX jobs must not be written to the hard disk drive.

5.1.2 Information Flow Control Policy (TSP_FLOW)

The security function "Information Flow" (TSF_FLOW) (see 2.3.2) restricts the information flow between the PSTN port of the optional FAX board (if installed) and the internal network by implementing a store-and-forward principle. The TOE does not allow information to flow between the PSTN port of the optional FAX processing board (if installed) and the network controller (which covers the information flow to and from the internal network). Data and/or commands cannot be sent to the internal network via the PSTN. A direct connection from the internal network to external entities by using the telephone line of the TOE is also denied.

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

- Only the copy controller (SIP) (see section 2.2) may copy image information and job data (e.g. the telephone number of the other fax machine) from and to a shared memory area on the FAX board.

- RECEIVING FAX: The FAX board must have terminated the PSTN connection before informing the copy controller about the fax currently received.

- SENDING FAX: The copy controller must have finished the copy operation of the fax image to the shared memory area of the FAX board before informing the FAX board to send the fax.

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

5.2 TOE Security Functional Requirements

5.2.1 Class FDP: User Data Protection

5.2.1.1 FDP_IFC.1 (1) Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] on [subjects: the hard disk drive information: image information operations: storage and erase of the image information].
Dependencies:	FDP_IFF.1 Simple security attributes

5.2.1.2 FDP_IFF.1 (1) Simple security attributes

Hierarchical to: No other components.

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

- MFD Job
  - Type of the job (print, network scan, scan to e-mail, copy, FAX)
- image information of the job
  - no security attributes

].

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

- A MFD job of the type print, network scan or scan to e-mail may store image information in the reserved space on the hard disk drive.

].

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

- When the TOE is turned back on after a power failure, all temporary document image data stored on the hard disk of abnormally terminated jobs shall be overwritten according to DoD 5200.28-M.
- Once the system administrator has invoked ODIO, the space on the hard disk drive reserved for temporary document image data shall be overwritten according to DoD 5200.28-M until the complete space is erased or the function is canceled by the system administrator.

].

FDP_IFF.1.4 The TSF shall provide [no additional SFP capabilities].

FDP_IFF.1.5	The TSF shall explicitly authorise an information flow based on the following rules: [none].
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: [• A MFD job of the type copy or fax must not store image information on the hard disk drive.].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

5.2.1.3 FDP_IFC.1 (2) Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the [information flow control policy TSP_FLOW] on [subjects: SIP, the network controller, the FAX board information: fax image information and job data, command messages operations: receiving a fax, sending command messages, receiving command messages, copy operation of FAX image data, sending a FAX].
Dependencies:	FDP_IFF.1 Simple security attributes

5.2.1.4 FDP_IFF.1 (2) Simple security attributes

Hierarchical to: No other components.

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

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

].

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

- The copy controller is allowed to copy fax image information and job data from the shared memory of the FAX board to its own memory.
- The copy controller is allowed to copy fax image information and job data from its own memory to the shared memory of the FAX board.

- The FAX board is allowed to send out a fax over PSTN once the copy controller has signaled the end of the copy operation to the shared memory area.
- The FAX board is allowed to signal the copy controller "Fax received" once the PSTN connection has been terminated.

].

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

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

].

FDP_IFF.1.4 The TSF shall provide [no additional SFP capabilities].

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [

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

].

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

5.2.1.5 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 **temporary image files will be overwritten according to DoD 5200.28-M** upon the *deallocation of the* ***temporary image files***

from the following objects: [print, network scan or scan to e-mail job].

Dependencies: No dependencies

Application Note: This SFR shall ensure that all temporary document image data written to the hard disk drive will be overwritten once the respective print, network scan or scan to e-mail job is finished.

5.2.2 Class FIA: Identification and Authentication

5.2.2.1 FIA_AFL.1 (1) Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [authentication at the local user interface in order to cancel ODIO].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lockout the SA login for a period of 2 minutes on the Local User Interface].

Dependencies: FIA_UAU.1 Timing of authentication

5.2.2.2 FIA_AFL.1 (2) Authentication failure handling

Hierarchical to: No other components

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [send the "403 Authorization Required" error code to this Browser session].

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: While the TOE will respond to every Web User Interface failed authentication attempt with the "403 Authorization Required" error code, is up to the web browser whether to display a message to the user or to re-attempt authentication. As of the time of this writing, Internet Explorer will re-prompt 3 times prior to displaying the error message whereas other browsers, such as Firefox, may re-prompt until the user

either enters the correct authentication information or clicks the "cancel" button in the authentication window and then display the error message.

5.2.2.3 FIA_AFL.1 (3) 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 at the local user interface].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lockout the SA login for a period of 3 minutes on the Local User Interface].
Dependencies:	FIA_UAU.1 Timing of authentication

5.2.2.4 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

5.2.2.5 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

5.2.2.6 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of Identification
FIA_UID.2.1	The TSF shall require each **system administrator** to identify itself before allowing any other TSF-mediated actions on behalf of that **system administrator**.
Dependencies:	No dependencies

5.2.3 Class FMT: Security Management

5.2.3.1 FMT_MSA.1 (1) Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] to restrict the ability to *change_default, modify, delete* [all] security attributes to [nobody].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

5.2.3.2 FMT_MSA.3 (1) Static attribute initialisation

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

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

5.2.3.3 FMT_MSA.1 (2) Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [information flow control policy TSP_FLOW] to restrict the ability to *change_default, query, modify, delete* [all] security attributes to [nobody].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

5.2.3.4 FMT_MSA.3 (2) Static attribute initialisation

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

Application Note: FMT_MSA.1 (2) and FMT_MSA.3 (2) requires the static initialization of the security attributes "Types of Command Messages between FAX board and copy controller", and the address spaces of these two objects. The TOE itself shall be able to initialize and manage these security attributes, so nobody shall be able to modify these values.

5.2.3.5 FMT_MOF.1 (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 [

- Immediate Image Overwrite (IIO),
- On Demand Image Overwrite (ODIO)

]

to [the system administrator].

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of management functions

5.2.3.6 FMT_MOF.1 (2) Management of Security Functions Behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to ***use*** the functions [

- Change PIN,
- Invoke ODIO,
- Abort ODIO

]

to [the system administrator].

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of management functions

5.2.3.7 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) [TSF_IOW] (Local User Interfaces),
- Enable/disable On Demand Image Overwrite (ODIO) [TSF_IOW] (Local User Interface),
- Change PIN (Local User Interface),
- Invoke ODIO [TSF_IOW] (Web and Local User Interfaces),
- Abort ODIO [TSF_IOW] (Web and Local User Interfaces)

]

Dependencies: No Dependencies

Application Note: When ODIO is invoked from the Web User Interface, it can only be cancelled at the Web User Interface. When ODIO is invoked from the Local User Interface, it can only be cancelled at the Local User Interface.

5.2.3.8 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

5.3 TOE Security Assurance Requirements

Table 8 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2, augmented with ALC_FLR3. The SARs are not iterated or refined from Part 3.

Table 8: EAL2 (augmented with ALC_FLR.3) 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

5.4 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

5.5 SFRs with SOF Declarations

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

FIA_UAU.2: Generally, the authentication mechanism has a PIN space of 12^3 – 12^{12} (3 – 12 digit PIN). Due to the security requirements of the Xerox guidance, the PIN size is defined as 8 to 12 digits (PIN Space of 12^8 to 12^{12}).

Justification for this metric can be found in section 8.6.

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 5.2.

- Image Overwrite (TSF_IOW)
- Authentication (TSF_AUT)
- Security Management (TSF_FMT)
- Information Flow (TSF_FLOW)

6.1.1 Image Overwrite (TSF_IOW)

The TOE implements an image overwrite security function (IIO) to overwrite temporary files created during the printing, network scan, or scan to e-mail 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 of the network controller. The definition of this reserved section is statically stored within the TOE and cannot be manipulated. Immediately after the job has completed, the files are overwritten using a three pass overwrite procedure as described in DoD 5200.28-M. Copy and FAX jobs do not get written to the HDD because they will not be processed by the network controller.

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

If ODIO was started from the Local UI and while ODIO is running, the Local UI will display a message stating that ODIO is in progress and an abort button. If ODIO was started from the Web UI and while ODIO is running, the Web UI will display a message stating that ODIO is in progress and an abort button. Before pressing the abort button, authentication as system administrator is required. If the System Administrator cancels ODIO, the process stops at a sector boundary. As part of the cancellation, the file system is rebuilt. This means, all temporary files are deleted but may not be overwritten as defined in DoD 5200.28-M. When ODIO is started from the Web UI, it can only be cancelled at the Web UI. Likewise, when ODIO is started from the Local UI, it can only be cancelled at the Local UI.

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

6.1.2 Information Flow (TSF_FLOW)

The TOE does not allow communication between the optional FAX processing board and the network controller and prevents therefore an interconnection between the PSTN and the internal network as illustrated in Figure 2.

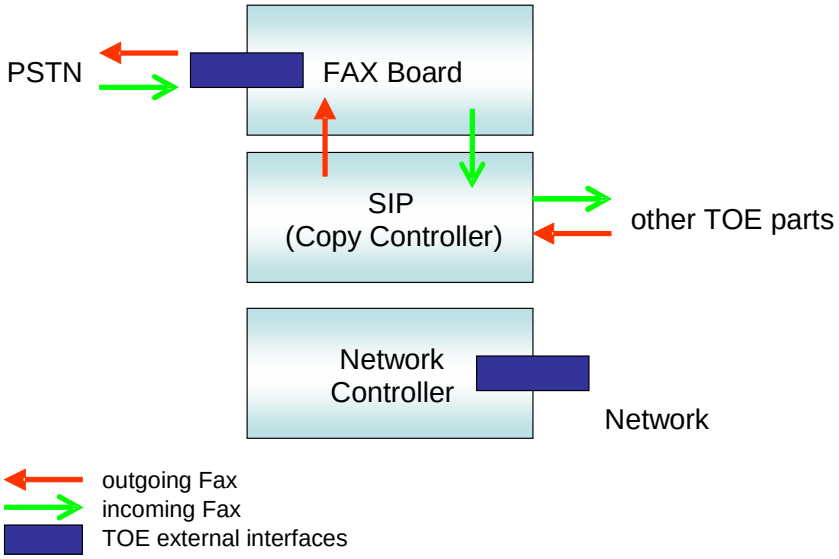

Figure 2: TSF_FLOW

There are two methods of communication between the copy controller and the FAX: Commands (which also includes the respective responses) and Image data transfer (which also includes job data like other FAX machines). Commands and responses are sent and received via a shared memory block on the FAX card by both the FAX card and the copy controller. Image data is also transferred in both directions using a shared memory area on the FAX card, but only by the copy controller.

For outgoing FAX the copy controller will push image data to the FAX card. The image data comes from the optical scanner. The copy controller will inform the FAX card when it has finished the transfer of the image data. The FAX card cannot access the shared memory area until the copy controller has completed its transfer of outgoing FAX image data. Likewise the copy controller cannot access the shared memory area until the FAX card has completed its transfer of incoming FAX image data.

For incoming FAX the FAX card will inform the copy controller when there is a FAX available for collection after the transmission of the fax has finished and the PSTN connection is

terminated. The copy controller will pull image data from the FAX card. The copy controller sends the image data only to the IOT software, which prints the FAX to paper.

The addresses of the shared memory areas of the FAX card and the types of command/response messages are statically defined within the TOE. No user or system administrator is able to change these values.

6.1.3 Authentication (TSF_AUT)

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

The authentication process for canceling an ODIO operation will be delayed at the Local User Interface, for 2 minutes if 5 wrong PINs were entered in succession (when attempting to cancel ODIO) or for 3 minutes if 3 wrong PINs were entered in succession (for any other authentication). If 1 wrong PIN is entered at the web interface from one particular Browser session, the TOE will send an error code ("HTTP 403 Authorization Required") to this Browser session. It will be up to the browser whether to display the message to the user or to re-prompt for authentication.

There are no more roles than "System Administrator" which can authenticate.

This security function is based on a probabilistic/permutational mechanism. The SOF claim is stated and justified in section 8.6.

6.1.4 Security Management (TSF_FMT)

The TOE provides some administrative functions to the system administrator. The following security management functions are provided by the TOE:

- Enable or Disable the Immediate Image Overwrite function (IIO) (Local User Interface only)
- Enable or Disable the On Demand Image Overwrite function (ODIO) (Local User Interface only)
- Change of the System Administrator PIN (via Local User Interface only)

- Invocation of ODIO (via Local User Interface or Web User Interface)
- Cancellation (Abort) of ODIO (via Web User Interface and Local User Interface)

Application Note: When ODIO is invoked from the Web User Interface, it can only be cancelled at the Web User Interface. When ODIO is invoked from the Local User Interface, it can only be cancelled at the Local User Interface. While IIO or ODIO can be disabled, doing so will remove the TOE from its evaluated configuration.

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, Life-Cycle, Testing, and Vulnerability Assessment Assurance Measures applied by Xerox to satisfy the CC EAL2, augmented with ALC_FLR.3, assurance requirements.

Table 9: Assurance Measures

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration Items	The vendor provides configuration management documents and a Configuration Item list.
ADO_DEL.1 Delivery Procedures	The vendor provides delivery procedures.
ADO_IGS.1 Installation, Generation and Startup procedures	The vendor provides secure installation, generation and start up procedures.
ADV_FSP.1 Informal function specification	The vendor provides an informal function specification.
ADV_HLD.1 Descriptive high-level design	The vendor provides 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 submits a system administration manual.
AGD_USR.1 User Guidance	The vendor submits a user guide.
ALC_FLR.3 Systematic flaw remediation	The vendor submits 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 is submits in the evaluation evidence.
ATE_FUN.1 Functional testing	The test evidence is submitted to the CCTL.

Assurance Component	How requirement will be met
ATE_IND.2 Independent testing - sample	The laboratory uses development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.
AVA_SOF.1 Strength of TOE security function evaluation	The vendor submits an analysis of the SOF for the PIN.
AVA_VLA.1 Developer vulnerability analysis	The vendor submits a vulnerability analysis.

7 PROTECTION PROFILE (PP) CLAIMS

The TOE does not claim conformance to a PP.

8 RATIONALE

8.1 Security Objectives Rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the assumptions to be met and identified threats to be countered.

Table 10: Security Objectives Rationale

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

Table 11: Security Objectives Rationale for the Environment

Assumption	Objective	Rationale
A.INSTALL	OE.INSTALL	OE.INSTALL covers A.INSTALL because the TOE will be delivered and installed by Xerox representatives according to all respective guidance documents. The TOE will be configured by the system administrator in accordance with the admin guidance of the TOE and the security guidance provided at the Xerox web site. This especially includes that the TOE is in the configuration under evaluation and that the Image Overwrite Security is installed and enabled. Furthermore, the default PIN was changed to a (at least) 8-digit PIN and the PIN will be changed at least every 40 days.
A.ACCESS	OE.ACCESS	OE.ACCESS covers A.ACCESS because the TOE will be installed in standard office environment and the office personnel will monitor the TOE to prevent unauthorized physical access to the HDD and the TOEs interfaces.
A.MANAGE	OE.ADMIN	OE.ADMIN covers A.MANAGE by requiring at least one trustworthy and responsible person to oversee the installation and operation of the TOE. This person(s) will be assigned according to onsite procedures and will follow all TOE administrator guidance. “Assignment” means here the person(s) get knowledge about the PIN.
A.NO_EVIL_ADM	OE.INSTALL OE.ADMIN	OE.ADMIN covers parts of A.NO_EVIL_ADM because “*responsible and trustworthy individual*” are “*not careless, willfully negligent or hostile*”. Furthermore, the individuals have to follow the instructions provided in the guidance documents. OE.INSTALL covers the remaining part of A.NO_EVIL_ADM because the objective ensures that the system administrator configures the TOE according to the configuration under evaluation and will not remove the TOE from its evaluated configuration (especially that the Image Overwrite Security accessory is installed and enabled).
A.NETWORK	OE.NETWORK	OE.NETWORK covers A.NETWORK by requiring a mechanism to detect network-based attacks against the TOE.

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 12: TOE SFR Mapping to Objectives

Objective	Rationale
O.RECOVER	FDP_RIP.1 ensures that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing. FDP_IFF.1 (1) together with FDP_IFC.1 (1) ensures that all temporary document image data of abnormally terminated jobs will be overwritten once the TOE is turned back on after a power failure. Additionally, these two requirements ensure that the complete space reserved for temporary document image data can be overwritten “on demand” by the system administrator. FMT_SMF.1 requires that there is a possibility to invoke this ODIO function. FMT_MOF.1 (2) restricts the access to this function to the system administrator. FMT_SMR.1 manages the role “system administrator”. FMT_MSA.3 (1) and FMT_MSA.1 (1) define the space where the temporary document image data can be stored and deny the modification of this space by anyone. FDP_IFF.1 (1) and FDP_IFC.1 (1) also ensure that Copy and Fax jobs will not be written to the HDD at all.
O.FAXLINE	FDP_IFC.1 (2) and FDP_IFF.1 (2) define the rules according to which an information flow between network controller, copy controller and FAX board (if installed) is allowed. By implementing a store-and-forward principle in both directions, a direct interconnection between the PSTN and the internal network is not possible.

Objective	Rationale
	FMT_MSA.3 (2) and FMT_MSA.1 (2) define the possible command types and the address spaces of the copy controller and the FAX board. Nobody shall be able to modify these parameters.
O.MANAGE	FMT_SMF.1 ensures that the security management functions (i.e., enable/disable IIO and ODIO, change system administrator PIN, and invoke/abort ODIO) are available on the TOE. FMT_MOF.1 (1) and FMT_MOF.1 (2) restrict the access to these management functions to the system administrator. FMT_SMR.1 manages the role "system administrator". FIA_UAU.2 and FIA_UID.2 ensure that system administrators are authenticated (and implicitly identified) before accessing the security functionality of the TOE. FIA_UAU.7 ensures that only obscured feedback generated by the authentication process is provided to system administrators before successful authentication. FIA_AFL.1 (1, 3) ensure that the TOE takes specific and immediate self-protection action when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Local User Interface. FIA_AFL.1 (2) provides an appropriate error message to the users web browser when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Web User Interface. Self-protection of the TOE is not possible due to the properties of a web interface (no dependable identification of the user's terminal and therefore no possibility to lock this terminal)

8.2.2 Rationale for Security Requirements for the Environment

There are not Security Requirements stated for the environment.

8.3 Rationale for the Assurance Level

This ST has been developed for multi-function digital image processing products incorporating an Image Overwrite Security option. The TOE environment will be exposed to only 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. ALC_FLR.3 ensures that instructions and procedures for the reporting, configuration management, and remediation of identified security flaws are in place and their inclusion is expected by the consumers of this TOE.

8.4 Rationale for TOE Summary Specification

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

The specified TSFs work together to satisfy the TOE SFRs. Table 13 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 13: Mapping of SFRs to Security Functions

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

TSF	SFR	Rational
	FIA_UID.2	TSF_AUT ensures that the system administrators must be identified (to include the implicit identification when the "Tools" menu is entered at the Local User Interface) before accessing the security functionality of the TOE.
	FIA_UAU.7	TSF_AUT ensures that only obscured feedback is generated by the authentication process.
	FIA_AFL.1 (1)	TSF_AUT ensures that the TOE locks the Local User Interface for 2 minutes if 5 unsuccessful authentication attempts happened at this user interface.
	FIA_AFL.1 (3)	TSF_AUT ensures that the TOE locks the Local User Interface for 3 minutes if 3 unsuccessful authentication attempts happened at this user interface.
	FIA_AFL.1 (2)	TSF_AUT ensures that the TOE provides an error message at the Web User Interface to a particular Browser session, if three unsuccessful authentication attempts happened from this Browser session.
	FMT_SMR.1	TSF_AUT only knows the role "system administrator".
TSF_FMT	FMT_SMF.1	TSF_FMT provides the security management functions enable/disable IIO and ODIO, change system administrator PIN, and invoke/abort ODIO
	FMT_MOF.1 (1) FMT_MOF.1 (2)	TSF_FMT restricts the access to these management functions to the system administrator.

8.5 TOE Assurance Requirements

Section 6.2 of this document identifies the Assurance Measures implemented by Xerox to satisfy the assurance requirements of EAL2, augmented with ALC_FLR.3, as delineated in the table in Annex B of the CC, Part 3. Table 14 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.3.

Table 14: 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**					

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Life Cycle	Test	Vulnerability Assessment
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**

8.6 TOE SOF Claims

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

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 the 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.

FIA_UAU.2 / TSF_AUT: This PIN space (12^8 to 12^{12}) is much larger than the PIN space a potential attacker with no or only low knowledge of the TOE and technical equipment can test in a reasonable amount of time. Therefore, this metric is appropriate for this attack potential and also complies with the SOF-basic claim.

8.7 Rationale for SFR and SAR Dependencies

Table 15 is a cross-reference of the functional components, their related dependencies, and whether the dependencies are satisfied.

Table 15: SFR Dependencies Status

Functional Component ID	Dependency (ies)	Satisfied
FDP_IFC.1 (1)	FDP_IFF.1	Yes, FDP_IFF.1 (1)
FDP_IFF.1 (1)	FDP_IFC.1	Yes, FDP_IFC.1 (1)
	FMT_MSA.3	Yes, FMT_MSA.3 (1)
FDP_IFC.1 (2)	FDP_IFF.1	Yes, FDP_IFF.1 (2)
FDP_IFF.1 (2)	FDP_IFC.1	Yes, FDP_IFC.1 (2)
	FMT_MSA.3	Yes, FMT_MSA.3 (2)
FDP_RIP.1	None	
FIA_AFL.1 (1)	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_AFL.1 (2)	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_AFL.1 (3)	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FIA_UAU.2	FIA_UID.1	Yes, hierarchically by FIA_UID.2. Identification of the system administrator at the Local User Interface is implicit -- the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window.
FIA_UAU.7	FIA_UAU.1	Yes, hierarchically by FIA_UAU.2
FMT_MOF.1 (1)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MOF.1 (2)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1 (1)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (1)
	FMT_SMR.1	No, because the authorized identified roles allowed to alter security attributes was defined as “Nobody”. So, no roles are required.
	FMT_SMF.1	No, because the authorized identified roles allowed to alter security attributes was defined as “Nobody”. So, no appropriate management functions are required.
FMT_MSA.3 (1)	FMT_MSA.1	Yes, FMT_MSA.1 (1)
	FMT_SMR.1	No, because the authorized identified roles allowed to specify alternative initial values was defined as “Nobody”. So, no roles are required.
FMT_MSA.1 (2)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (2)
	FMT_SMR.1	No, because the authorized identified roles allowed to alter security attributes was defined as “Nobody”. So, no roles are required.

Functional Component ID	Dependency (ies)	Satisfied
	FMT_SMF.1	No, because the authorized identified roles allowed to alter security attributes was defined as “Nobody”. So, no appropriate management functions are required.
FMT_MSA.3 (2)	FMT_MSA.1	Yes, FMT_MSA.1 (2)
	FMT_SMR.1	No, because the authorized identified roles allowed to specify alternative initial values was defined as “Nobody”. So, no roles are required.
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Yes, hierarchically by FIA_UID.2. Identification of the system administrator at the Local User Interface is implicit -- the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window.

SAR dependencies identified in the CC have been met by this ST as shown in Table 16.

Table 16: EAL2 (Augmented with ALC_FLR.3) SAR Dependencies Satisfied

Assurance Component ID	Dependencies	Satisfied
ACM_CAP.2	None	
ADO_DEL.1	None	
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1	Yes
	ADV_RCR.1	Yes
ADV_RCR.1	None	
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ALC_FLR.3	None	
ATE_COV.1	ADV_FSP.1	Yes
	ATE_FUN.1	Yes
ATE_FUN.1	None	
ATE_IND.2	ADV_FSP.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes
	ATE_FUN.1	Yes
AVA_SOF.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes

8.8 Internal Consistency and Mutually Supportive Rationale

8.8.1 Internal Consistency

The SARs represent EAL2 augmented with ALC_FLR.3. The EAL2 SARs are internally consistent because SARs within an EAL, by definition, do not conflict with each other. The ALC_FLR.3 SAR, while not contained within any EAL, operates independently of all other SARS (it has no dependencies), and does not conflict with the SARs included in EAL2.

The set of SFRs and set of SARs in this Security Target are completely independent of each other; therefore, no inconsistencies are present between them. There is no conflict between the security functions, as described in Section 2 and Section 6, and the SARs which could prevent satisfaction of all SFRs.

The security objectives do not conflict with each other because they have completely different aims. The rationale shows that each of the security objectives is met by its assigned SFRs.

Therefore the SFRs assigned to one security objective will necessarily not conflict with the SFRs assigned to another because the objectives concern different operations, events and/or data.

8.8.2 Mutually Supportive Whole

The choice of security requirements is justified as shown in Sections 8.2 and 8.3. 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 the threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 15 and Table 16 and described in Section 8.7.

- The security functions TSF_FLOW is a completely TOE internal security function and cannot be bypassed, tampered or de-activated by other security functions.

- The security function TSF_IOW can only be de-activated by the system administrator. TSF_FMT and TSF_AUT prevent this. If TSF_IOW is activated, bypassing or tampering is not possible.

- TSF_FMT provides some security functions and TSF_AUT prevents the usage of these functions for all users than-system administrators.

- Due to the fact that the security functions are a mutually supportive whole and the underlying SFRs are internal consistent, the SFR must also be a mutually supportive whole.