

**THE DOCUMENT COMPANY**

**XEROX®**

**Image Overwrite Security**

**for the**

**Xerox WorkCentre M35/M45/M55**

**and**

**WorkCentre Pro 35/45/55**

**Advanced Multifunction System**

**Security Target**

**Version 1.0**

**Prepared by:**



Xerox Corporation  
250 Cross Keys Office Park  
Fairport, New York 14450

Computer Sciences Corporation  
132 National Business Parkway  
Annapolis Junction, MD 20701

<b>Date</b>	<b>Revision</b>	<b>Changes Made</b>
May 16, 2003	0.1	Original Draft
June 18, 2003	0.2	Incorporated Xerox comments
June 20, 2003	0.3	Made fax component optional.
June 20, 2003	0.9	Made Xerox changes to detail what is erased and when
June 23, 2003	0.10	Make minor capitalization changes.
July 14, 2003	0.11	Added WorkCentre to WorkCentre Pro
July 23, 2003	0.12	Addressed EDR_001
July 24, 2003	0.13	Internal review
July 24, 2003	0.14	Fixed QA comments.
July 31, 2003	1.3	Addressed EDR_002 – added to cvs and changed version to 1.3
August 1, 2003	1.4	Removed FDP_ACC and FDP_ACF and replaced with Explicitly Stated Requirement EXP_FAX
August 4, 2003	1.5	Fixed T.FAXLINE to account for telephone line/modem
August 5, 2003	1.6	Updated the TSS, fixed footer (date and revision), updated FMT_MOF.1 and FMT_SMF.1
August 6, 2003	1.7	Updated EXP_FAX.1.1 and Rational for Explicitly stated requirement
August 7, 2003	1.8	Updated Table 2 – Evaluated Software/Firmware version
August 18, 2003	1.9	Rework TSS TSF_IOW and TSF_FLOW
September 2, 2003	1.10	Incorporate comments
September 3, 2003	1.11	Re-work Table 2 – Evaluated Software/Firmware version to match ordering and style used in Configuration Report from Device
September 16, 2003	1.12	Added abort to FMT_SMF.1
September 19, 2003	1.13	Corrections to FMT_SMF.1.1
October 2, 2003	1.14	Added FIA_UID.1
October 3, 2003	1.15	Updated TSF_FMT to reflect the web interface
October 15, 2003	1.16	Updates to reflect editorial changes by Xerox
November 18, 2003	1.17	Added change PIN
December 4, 2003	1.18	Modified change PIN to TSF_FMT
December 17, 2003	1.19	Revised S/W version table
January 8, 2004	1.20	Updated version table for patch level upgrade
January 8, 2004	1.21	Revised version table for patch level P2
January 22, 2004	1.22	Revised version table for patch level P3
February 11, 2004	1.23	Revised version table.
February 18, 2004	1.24	Changed UID.1 to UID.2 in table 11 updated revision marks.
March 17, 2004	1.25	Changed Firmware version numbers for SMP2 release.
April 16, 2004	1.27	Changed Firmware version numbers for SMP1 P4, P5.

# Table of Contents

---

<b>1</b>	<b>SECURITY TARGET INTRODUCTION .....</b>	<b>1</b>
1.1	ST AND TOE IDENTIFICATION .....	1
1.2	REFERENCES .....	2
1.3	CONVENTIONS, TERMINOLOGY, AND ACRONYMS .....	2
1.3.1	<i>Conventions</i> .....	2
1.3.2	<i>Terminology</i> .....	3
1.3.3	<i>Acronyms</i> .....	4
1.4	TOE OVERVIEW .....	5
1.5	COMMON CRITERIA CONFORMANCE CLAIM .....	5
<b>2</b>	<b>TOE DESCRIPTION.....</b>	<b>6</b>
2.1	PRODUCT TYPE.....	6
2.1.1	<i>Physical Scope and Boundary</i> .....	7
2.1.2	<i>Logical Scope and Boundary</i> .....	7
<b>3</b>	<b>TOE SECURITY ENVIRONMENT.....</b>	<b>9</b>
3.1	SECURE USAGE ASSUMPTIONS .....	9
3.1.1	<i>Environment Assumptions</i> .....	9
3.2	THREATS .....	9
3.3	ORGANIZATIONAL SECURITY POLICIES .....	10
<b>4</b>	<b>SECURITY OBJECTIVES.....</b>	<b>11</b>
4.1	SECURITY OBJECTIVES FOR THE TOE.....	11
4.2	SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	11
<b>5</b>	<b>IT SECURITY REQUIREMENTS .....</b>	<b>12</b>
5.1	TOE SECURITY FUNCTIONAL REQUIREMENTS .....	12
5.1.1	<i>Class FDP: User Data Protection</i> .....	12
5.1.2	<i>Class FIA: Identification and Authentication</i> .....	13
5.1.3	<i>Class FMT: Security Management</i> .....	13
5.2	TOE SECURITY ASSURANCE REQUIREMENTS.....	14
5.3	SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT .....	15
5.4	EXPLICITLY STATED REQUIREMENTS FOR THE TOE.....	15
5.5	SFRs WITH SOF DECLARATIONS.....	15
<b>6</b>	<b>TOE SUMMARY SPECIFICATION .....</b>	<b>16</b>
6.1	TOE SECURITY FUNCTIONS.....	16
6.1.1	<i>Image Overwrite (TSF_IOW)</i> .....	16
6.1.2	<i>Information Flow (TSF_FLOW)</i> .....	16
6.1.3	<i>Authentication (TSF_AUT)</i> .....	17
6.1.4	<i>Security Management (TSF_FMT)</i> .....	17
6.2	ASSURANCE MEASURES .....	18
<b>7</b>	<b>PROTECTION PROFILE (PP) CLAIMS.....</b>	<b>19</b>

---

<b>8</b>	<b>RATIONALE.....</b>	<b>20</b>
8.1	SECURITY OBJECTIVES RATIONALE.....	20
8.2	SECURITY REQUIREMENTS RATIONALE.....	21
8.2.1	<i>Rationale For TOE Security Requirements</i> .....	22
8.3	RATIONALE FOR ASSURANCE LEVEL.....	23
8.4	RATIONALE FOR TOE SUMMARY SPECIFICATION.....	23
8.4.1	<i>TOE Assurance Requirements</i> .....	24
8.4.2	<i>TOE SOF Claims</i> .....	25
8.5	RATIONALE FOR SFR AND SAR DEPENDENCIES.....	25
8.6	RATIONALE FOR EXPLICITLY STATED REQUIREMENTS.....	26
8.7	INTERNAL CONSISTENCY AND MUTUALLY SUPPORTIVE RATIONALE.....	27

## List of Figures

---

Figure 1: Xerox WorkCentre/WorkCentre Pro 35/45/55.....	7
---	---

## List of Tables

---

Table 1: Models and capabilities .....	6
Table 2: Evaluated Software/Firmware version .....	7
Table 3: Environmental Assumptions.....	9
Table 5: Threats to the TOE.....	10
Table 7: Security Objectives for the TOE.....	11
Table 9: Security Objectives for the TOE Environment.....	11
Table 11: TOE Security Functional Requirements.....	12
Table 13: EAL2 Assurance Requirements.....	14
Table 15: Security Objectives Rationale.....	20
Table 16: Security Objectives Rationale for the Environment .....	21
Table 17: TOE SFR Mapping to Objectives.....	23
Table 18: Mapping of SFRs to Security Functions.....	23
Table 20: Assurance Measure Compliance Matrix.....	24
Table 22: SFR Dependencies Status .....	25
Table 24: EAL2 SAR Dependencies Satisfied .....	26

# 1 SECURITY TARGET INTRODUCTION

- 1 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).
- 2 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

- 3 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.

<b>ST Title:</b>	Image Overwrite Security for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System Security Target
<b>ST Version:</b>	1.0
<b>Revision Number:</b>	\$Revision: 1.27 \$
<b>Publication Date:</b>	\$Date: 2004/04/16 08:15:59 \$
<b>Authors:</b>	Computer Sciences Corporation, Common Criteria Testing Laboratory
<b>TOE Identification:</b>	Xerox WorkCentre M35/M45/M55 / WorkCentre Pro 35/45/55 Advanced Multifunction System with Image Overwrite Security option.
<b>CC Identification:</b>	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408)
<b>ST Evaluator:</b>	Computer Sciences Corporation (CSC)
<b>Keywords:</b>	Xerox, Multi Function Device, Image Overwrite

## 1.2 References

4 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 1999, version 2.1, CCIMB-99-031, Incorporated with interpretations as of 2002-02-28
- [CC\_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032 , Incorporated with interpretations as of 2002-02-28.
- [CC\_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033, Incorporated with interpretations as of 2002-02-28.
- [CEM\_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.
- [CEM\_PART2] Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

## 1.3 Conventions, Terminology, and Acronyms

5 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

6 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.

7 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 (1) and FMT\_MTD.1.1 (2).
- e) Plain *italicized text* is used to emphasize text.

### 1.3.2 Terminology

8 In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

<b><i>Authentication data</i></b>	Information used to verify the claimed identity of a user.
<b><i>Authorized User</i></b>	A user who may, in accordance with the TOE Security Policy (TSP <sup>1</sup> ), perform an operation.
<b><i>External IT entity</i></b>	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
<b><i>Human user</i></b>	Any person who interacts with the TOE.
<b><i>Identity</i></b>	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.
<b><i>Object</i></b>	An entity within the TOE Security Function (TSF <sup>2</sup> ) Scope of Control (TSC <sup>3</sup> ) that contains or receives information and upon which subjects perform operations.
<b><i>Role</i></b>	A predefined set of rules establishing the allowed interactions between a user and the TOE.
<b><i>Security Functional Components</i></b>	Express security requirements intended to counter threats in the assumed operating environment of the TOE.
<b><i>Subject</i></b>	An entity within the TSC that causes operations to be performed.
<b><i>User</i></b>	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

9 The following terminology is specific to this ST.

<b><i>Image Data</i></b>	Information on a mass storage device created by the copy/print/scan/FAX/email process.
--------------------------	--

---

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.

---

***Latent Image Data***      Residual information remaining on a mass storage device when a copy/print/scan/FAX/email job is completed, cancelled, or interrupted.

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

### 1.3.3 Acronyms

10      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
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
ISO	International Standards Organization
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
MOF	Management of Functions
MTD	Management of TSF Data
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication

ACRONYM	DEFINITION
UDP	User Data Protection

## 1.4 TOE Overview

- 11 The TOE is a multi-function device (copy & print), with scan to e-mail, network scan and FAX, options (hereafter referred to as a MFD). An additional optional component is the Image Overwrite Security package. This option forces any temporary image files created during a print, network scan, or scan to email job to be erased when those files are no longer needed or “on demand” by the system administrator.
- 12 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

- 13 This ST conforms to CC Part 2 extended, and is CC Part 3 conformant at the EAL 2 level of assurance.

## 2 TOE DESCRIPTION

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

### 2.1 Product Type

15 The TOE is a multi-function device that copies and prints, with scan to e-mail, network scan and FAX, options (hereafter referred to as a MFD). An additional optional component is the Image Overwrite Security package. This option forces any temporary image files created during a print, network scan, or scan to email job to be erased when those files are no longer needed.

**Table 1: Models and capabilities**

	Print	Copy <sup>1</sup>	Network Scan	FAX <sup>1</sup>	Scan 2 email
WorkCentre M35	x	x	n/a	o	o
WorkCentre M45	x	x	n/a	o	o
WorkCentre M55	x	x	n/a	o	o
WorkCentre Pro 35	x	x	o	o	o
WorkCentre Pro 45	x	x	o	o	o
WorkCentre Pro 55	x	x	o	o	o

<sup>1</sup> Copy and FAX jobs are not spooled to the HDD.

16 A MFD stores temporary image data created during a print, network scan or scan to email 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. Copy and FAX jobs do not get written to the HDD.

17 The TOE provides an IMAGE\_OVERWRITE (TSF\_IOW) 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 email 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 decommissioned, for example.

### 2.1.1 Physical Scope and Boundary

18 The TOE is a Multi-Function Device that consists of a printer, copier, scanner, FAX, and email as shown in Figure 1.



19 The figure shows an optional paper feeder and finisher.

**Table 2: Evaluated Software/Firmware version**

Software/Firmware Item	WorkCentre M35/M45/M55	WorkCentre M35/M45/M55 + PostScript	WorkCentre Pro 35/45/55
System Software	2.84.16.000	4.84.16.000	3.84.16.000
Network Controller Software	1.02.129.1.P4.P5	1.02.229.1.P4.P5	1.02.329.1.P4.P5
UI Software	002.84.014	002.84.014	002.84.014
SIP Software	10.84.2	10.84.2	10.84.2
IOT Software	23.16.000	23.16.000	23.16.000
DADH Software	12.15.00	12.15.00	12.15.00
Finisher Software	09.15.00	09.15.00	09.15.00
FAX Software	00.84.15	00.84.15	00.84.15

### 2.1.2 Logical Scope and Boundary

20 The TOE logical boundary is the following security functions controlled by the TOE:

- Image Overwrite (TSF\_IOW)
- Authentication (TSF\_AUT)
- Security Management (TSF\_FMT)
- Data Flow Security (TSF\_FLOW)

21 During normal operation, the MFD spools temporary document image data to a HDD. The image overwrite function (TSF\_IOW) clears temporary document image data from the HDD by

*Security Target for the Xerox Image Overwrite Security*

writing over the image data with three specific patterns of data. The image overwrite function clears data once a job is completed or when invoked at any time by the system administrator.

- 22 Only users who are assigned as the system administrator and authenticated via a personal identification number (PIN) (TSF\_AUT) can access the security settings of the MFD (TSF\_FMT). Any user can utilize the other non-security-related features/functions of the MFD without authentication.
- 23 TSF\_FLOW ensures that a malicious user cannot access network resources from the telephone line via the TOE's FAX modem.

### 3 TOE SECURITY ENVIRONMENT

#### 3.1 Secure Usage Assumptions

24 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.

25 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

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

**Table 3: Environmental Assumptions**

Assumption	Description
A.INSTALL	The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
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_KOC	System administrators PIN is changed according to the following: 8-digit PIN every 40 days 9-digit PIN every year

#### 3.2 Threats

27 Table 4 identifies the threats to the TOE. The threats to the TOE 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 threat has 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 from a print/network scan/email 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.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).

### 3.3 Organizational Security Policies

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

## 4 SECURITY OBJECTIVES

29 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

30 This section identifies and describes the security objectives of the TOE.

31 The TOE accomplishes the security objectives defined in Table 5.

**Table 5: Security Objectives for the TOE**

Objectives	Description
O.RESIDUAL	Temporary document image data from a job must not remain on the hard disk drive once that job is completed.
O.MANAGE	Only System Administrators shall have the capability to exercise security management functions provided by the TSF.
O.RESTRICT	The TOE will restrict 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."

### 4.2 Security Objectives for the Environment

32 The security objectives for the IT Environment are defined in Table 6.

**Table 6: Security Objectives for the TOE Environment**

Objectives	Description
OE.MANAGE	A responsible individual will be assigned as the system administrator who will see that the TOE is installed, and is operated in accordance with all applicable policies and procedures necessary to operate the TOE in a secure manner.

## 5 IT SECURITY REQUIREMENTS

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

34 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).

35 These requirements are discussed separately within the following subsections.

### 5.1 TOE Security Functional Requirements

36 The TOE satisfies the SFRs delineated in Table 7. The rest of this section contains a description of each component and any related dependencies.

**Table 7: TOE Security Functional Requirements**

Functional Component ID	Functional Component Name
FDP_RIP.1	Subset Residual Information Protection
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_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles

#### 5.1.1 Class FDP: User Data Protection

37 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

### 5.1.2 Class FIA: Identification and Authentication

38 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

39 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

40 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

### 5.1.3 Class FMT: Security Management

41 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] to [the system administrator].

Dependencies: FMT\_SMR.1 Security Roles  
FMT\_SMF.1 Specification of management functions

42 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],  
 Change PIN,  
 Invoke/Abort ODIO [TSF\_IOW]

Dependencies: No Dependencies

43 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

44 Application Note: The TOE does not support FIA\_UID.1 directly. Please see the Security Functional Rationale for additional details.

## 5.2 TOE Security Assurance Requirements

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

**Table 8: 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
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

Assurance Component ID	Assurance Component Name	Dependencies
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

46 There are no security functional requirements for the IT Environment.

### 5.4 Explicitly Stated Requirements for the TOE

47 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

### 5.5 SFRs With SOF Declarations

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

49 FIA\_UAU.2: The authentication mechanism has a PIN space of  $10^3 - 10^{12}$  (3 – 12 digit PIN). Through Xerox guidance, the recommend PIN size is 8 to 12 digits (PIN Space of  $10^8$  to  $10^{12}$ ).

## 6 TOE SUMMARY SPECIFICATION

50 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

51 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.

#### 6.1.1 Image Overwrite (TSF\_IOW)

52 The TOE implements an image overwrite security function to erase temporary files created during the printing, network scan, or scan to email 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 5800.28-M (Immediate Image Overwrite (IIO) and "On-Demand" Image Overwrite (ODIO)). The TSF\_IOW function can also be invoked manually by the system administrator (ODIO).

53 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.

54 While ODIO is running, the GUI will display a message stating that ODIO is in progress and a 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.

55 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.

56 **Functional Requirements Satisfied:** FDP\_RIP.1

#### 6.1.2 Information Flow (TSF\_FLOW)

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

58 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

59 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.

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

61 **Functional Requirements Satisfied:** EXP\_FAX.1

### 6.1.3 Authentication (TSF\_AUT)

62 The TOE utilizes a simple authentication function through the front panel or web interface. The  
system administrator must authenticate by entering an 3 to 12 digit PIN 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  $10^3$  to  $10^{12}$ .

63 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, but is provided for historical  
reasons. 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  
privileges based on username.

64 **Functional Requirements Satisfied:** FMT\_SMR.1, FIA\_UAU.2, FIA\_UAU.7, FIA\_UID.2

### 6.1.4 Security Management (TSF\_FMT)

65 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.

66 Additionally, TSF\_FMT utilizes the web server authentication mechanism to allow only  
authenticated system administrators the capability to manually invoke "On Demand" Image  
Overwrite through the web interface.

67 The TOE restricts access to the configuration of administrative functions to the system  
administrator.

68 **Functional Requirements Satisfied:** FMT\_SMR.1, FMT\_MOF.1, FMT\_SMF.1

## 6.2 Assurance Measures

69 The TOE satisfies CC EAL2 assurance requirements. 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.
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.
AVA_VLA.2 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**

70 The TOE does not claim conformance to a PP.

## 8 RATIONALE

71 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

72 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 9: Security Objectives Rationale**

Objective	Threat Organizational Security Policy Assumption	Rational
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

Objective	Threat Organizational Security Policy Assumption	Rational
		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.

**Table 10: Security Objectives Rationale for the Environment**

Objective	Threat Organizational Security Policy Assumption	Rational
OE.MANAGE	A.CHANGE_KOC A.INSTALL A.MANAGE A.NO_EVIL_ADM A.PROCEDURE	OE.MANAGE is met by A.CHANGE_KOC, A.INSTALL, A.MANAGE, A.NO_EVIL_ADM, A.PROCEDURE by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE.

## 8.2 Security Requirements Rationale

73

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

74 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

75 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.

SFR	Rationale
FDP_RIP.1	Ensures that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing. This SFR traces back and meets O.RESIDUAL and O.ONDEMAND.
FIA_UID.2	Ensures that system administrators are authenticated before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FIA_UAU.2	Ensures that system administrators are authenticated before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FIA_UAU.7	Ensures that only obscured feedback generated by the authentication process is provided to system administrators before successful authentication. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FMT_MOF.1	Ensures that only system administrators have the capability to enable, disable, or manually invoke the Security Mode SFR. This SFR traces back and aids in meeting the following objective: O.MANAGE.
FMT_SMF.1	Defines the set of security functions available on the TOE. Specifically a dependency for FMT_SMR.1 and O.ONDEMAND.
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.
EXP_FAX.1	Network FAX separation protects TSF and its data from modification or tampering. O.RESTRICT is met by 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.

**Table 11: TOE SFR Mapping to Objectives**

	O.RESIDUAL	O.RESTRICT	O.MANAGE	O.ONDEMAND
FDP_RIP.1	X			X
FIA_UAU.2			X	
FIA_UAU.7			X	
FMT_UID.2			X	
FMT_MOF.1			X	
FMT_SMF.1				X
FMT_SMR.1			X	X
EXP_FAX.1		X		

### 8.3 Rationale For Assurance Level

76 This ST has been developed for multi-function digital image processing products incorporating a Image Overwrite Security option. 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.

### 8.4 Rationale For TOE Summary Specification

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

78 The specified TSFs work together to satisfy the TOE SFRs. Table 12 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

**Table 12: Mapping of SFRs to Security Functions**

SFR	Name	TSF	Name
FDP_RIP.1	Subset Residual Information Protection	TSF_IOW	Image Overwrite
FIA_UAU.2	User Authentication before any Action	TSF_AUT	Authentication

SFR	Name	TSF	Name
FIA_UAU.7	Protected Authentication Feedback	TSF_AUT	Authentication
FIA_UID.2	User identification before any action	TSF_AUT	Authentication
FMT_MOF.1	Management of Security Functions Behavior (1)	TSF_FMT	Security Management
FMT_SMF.1	Specification of Management Functions	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_AUT	Authentication
EXP_FAX.1	Network FAX Separation	TSF_FLOW	Information Flow

### 8.4.1 TOE Assurance Requirements

79

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 13 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

**Table 13: Assurance Measure Compliance Matrix**

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	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		
ATE_COV.1					X	
ATE_FUN.1					X	
ATE_IND.2					X	
AVA_SOF.1						X

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
AVA_VLA.1						X

### 8.4.2 TOE SOF Claims

80 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

81 Table 14 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

**Table 14: SFR Dependencies Status**

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FDP_RIP.1	Residual Information Protection	None	
FIA_UAU.2	User Authentication before any Action	FIA_UID.1	Yes
FIA_UAU.7	Protected Authentication Feedback	FIA_UAU.1	Yes
FIA_UID.2	User identification before any action	none	
FMT_MOF.1	Management of Security Functions Behavior	FMT_SMF.1 FMT_SMR.1	Yes
FMT_SMF.1	Specification of Management Functions	None	
FMT_SMR.1	Security Roles	FIA_UID.1	Yes

82 SAR dependencies identified in the CC have been met by this ST as shown in Table 15.

**Table 15: 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
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

- 83 The CC is geared toward operating systems, as such, FPT\_SEP.1 does not fit the TOE's architecture. 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.

## **8.7 Internal Consistency and Mutually Supportive Rationale**

84 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 12. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 14 and Table 15 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 13. 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.