Xerox WorkCentre

4150 / 4150s / 4150x / 4150xf 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

1 SECURITY TARGET INTRODUCTION 1
1.1 ST AND TOE IDENTIFICATION 1
1.2 REFERENCES 2
1.3 CONVENTIONS, TERMINOLOGY, AND ACRONYMS 2
1.3.1 Conventions 2
1.3.2 Terminology 3
1.3.3 Acronyms 4
1.4 TOE OVERVIEW 5
1.5 COMMON CRITERIA CONFORMANCE CLAIM 5
2 TOE DESCRIPTION 6
2.1 PRODUCT TYPE 6
2.2 PHYSICAL SCOPE AND BOUNDARY 7
2.3 LOGICAL SCOPE AND BOUNDARY 8
2.3.1 Image Overwrite (TSF_IOW) 9
2.3.2 Information Flow (TSF_FLOW) 9
2.3.3 System Authentication (TSF_SYS_AUT) 9
2.3.4 Network Authentication (TSF_NET_AUT) 9
2.3.5 Security Audit (TSF_FAU) 10
2.3.6 Cryptographic Operations (TSF_FCS) 10
2.3.7 User Data Protection – SSL (TSF_FDP_SSL) 10
2.3.8 User Data Protection – IP Filtering (TSF_FDP_FILTER) 10
2.3.9 Security Management (TSF_FMT) 11
2.4 TOE SECURITY ARCHITECTURE (TSF_ARCH) 11
2.5 EVALUATED CONFIGURATION 11
3 TOE SECURITY ENVIRONMENT 12
3.1 ASSUMPTIONS 12
3.2 THREATS 13
3.2.1 Threats Addressed by the TOE 13
3.2.2 Threats Addressed by the IT Environment 15
3.3 ORGANIZATIONAL SECURITY POLICIES 15
4 SECURITY OBJECTIVES 17
4.1 SECURITY OBJECTIVES FOR THE TOE 17
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 18
4.2.1 Security objectives for the IT Environment 18
4.2.2 Security objectives for the non IT Environment 18
5 IT SECURITY REQUIREMENTS 20
5.1 SECURITY POLICIES 20
5.1.1 User Data Protection Policy (TSP_IOW) 20

5.1.2 Information Flow Control Policy (TSP_FLOW) 21
5.1.3 SSL SFP (TSP_SSL) 21
5.1.4 IP Filter SFP (TSP_FILTER) 21
5.1.5 Privileged User Access SFP (TSP_FMT) 22
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 22
5.2.1 Class FAU: Security Audit 22
5.2.2 Class FCS: Cryptographic Support 25
5.2.3 Class FDP: User Data Protection 29
5.2.4 Class FIA: Identification and Authentication 37
5.2.5 Class FMT: Security Management 39
5.2.6 Class FPT: Protection of the TSF 45
5.2.7 Class FTP: Trusted path/channels 46
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 48
5.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 49
5.5 SFRS WITH SOF DECLARATIONS 49
6 TOE SUMMARY SPECIFICATION 50
6.1 TOE SECURITY FUNCTIONS 50
6.1.1 Image Overwrite (TSF_IOW) 50
6.1.2 Information Flow (TSF_FLOW) 51
6.1.3 Authentication (TSF_SYS_AUT) 52
6.1.4 Network Authentication (TSF_NET_AUT) 52
6.1.5 Security Audit (TSF_FAU) 53
6.1.6 Cryptographic Support (TSF_FCS) 54
6.1.7 User Data Protection – SSL (TSF_FDP_SSL) 54
6.1.8 User Data Protection – IP Filtering (TSF_FDP_FILTER) 55
6.1.9 Security Management (TSF_FMT) 55
6.1.10 TOE Security Architecture (TSF_ARCH) 55
6.2 ASSURANCE MEASURES 55
7 PROTECTION PROFILE (PP) CLAIMS 58
8 RATIONALE 59
8.1 SECURITY OBJECTIVES RATIONALE 59
8.2 SECURITY REQUIREMENTS RATIONALE 62
8.2.1 Rationale For TOE Security Requirements 62
8.2.2 Rationale for Security Requirements for the Environment 66
8.3 RATIONALE FOR THE ASSURANCE LEVEL 66
8.4 RATIONALE FOR TOE SUMMARY SPECIFICATION 67
8.5 TOE ASSURANCE REQUIREMENTS 72
8.6 TOE SOF CLAIMS 73
8.7 RATIONALE FOR SFR AND SAR DEPENDENCIES 74
8.8 INTERNAL CONSISTENCY AND MUTUALLY SUPPORTIVE RATIONALE 80
8.8.1 Internal Consistency 80
8.8.2 Mutually Supportive Whole 81

List of Figures

Figure 1: Xerox WorkCentre 4150 / 4150s / 4150x / 4150xf 7
Figure 2: TSF_FLOW 51

List of Tables

Table 1: Models and capabilities 6
Table 2: Evaluated Software/Firmware version 8
Table 3: Environmental Assumptions 12
Table 4: Threats to the TOE 14
Table 5: Threat Addressed by the IT Environment 15
Table 6: Organizational Security Policy(s) 15
Table 7: Security Objectives for the TOE 17
Table 8: Security Objectives for the IT Environment 18
Table 9: Security Objectives for the non-IT Environment 18
Table 10: Audit Events 22
Table 11: EAL3 (augmented with ALC_FLR.3) Assurance Requirements 48
Table 12: Assurance Measures 56
Table 13: Security Objectives Rationale (Threats) 59
Table 14: Security Objectives Rationale (Assumptions and OSPs) 60
Table 15: TOE SFR Mapping to Objectives 62
Table 16: Mapping of SFRs to Security Functions 67
Table 17: Assurance Measure Compliance Matrix 73
Table 18: SFR Dependencies Status 74
Table 19: EAL3 (Augmented with ALC_FLR.3) SAR Dependencies Satisfied 80

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) 3, augmented with ALC_FLR.3.

ST Title:	Xerox WorkCentre 4150 / 4150s / 4150x / 4150xf Multifunction Systems Security Target
ST Version:	1.0
Revision Number:	Revision 1.06
Publication Date:	April 6, 2009
Authors:	Computer Sciences Corporation (US) Common Criteria Testing Laboratory, Xerox Corporation
Sponsor:	Xerox Corporation
TOE Identification:	Xerox WorkCentre 4150 / 4150s / 4150x / 4150xf 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.
Image Data	Information on a mass storage device created by the copy (landscape/stapled type only)/print/scan/e-mail process.
Latent Image Data	Residual information remaining on a mass storage device when a copy (landscape/stapled type only)/print/scan/ e-mail job is completed, cancelled, or interrupted.

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.

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.

1.3.3 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
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
SM	Security Management
SMF	Security Management Functions (CC Family)
SMR	Security Management Roles (CC Family)
SOF	Strength of Function
ST	Security Target

ACRONYM	DEFINITION
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
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 on the hard disk drive (HDD) during a copy (landscape/stapled type only), 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 FAX jobs are not written to the HDD, there are no temporary images files to be overwritten for this service.

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, EAL3 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 on the HDD during a copy (landscape/stapled type only), print, network scan, or scan to e-mail job to be overwritten when those files are no longer needed.

The optional Xerox 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; n/a - not available)

	Print	Copy[1]	Network Scan	FAX[1]	Scan to e-mail	Print Speed
WorkCentre 4150	n/a	X	n/a	n/a	n/a	Up to 45ppm
WorkCentre 4150s	X	X	o	o	o	Up to 45ppm
WorkCentre 4150x	X	X	o	X	o	Up to 45ppm
WorkCentre 4150xf	X	X	o	X	o	Up to 45ppm

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

A MFD stores temporary image data created during a copy (landscape/stapled type only), 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 FAX jobs are not written to the HDD, there are no temporary images files to be overwritten for this service.

NOTE: Print, network scan and scan to e-mail jobs are written directly to the HDD when the job enters the system. Copy jobs are buffered in volatile memory with one exception: only copy jobs of type "landscape/stapled" are written to the disk. Any data that gets written to the disk will be overwritten at the completion of the job.

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[4] at the completion of each copy (landscape/stapled type only), 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 models 4150, 4150s, 4150x or 4150xf) that consists of a copier and the following additional options when purchased by the consumer: printer, scanner, FAX, and scan-to e-mail. All models of the TOE include Administrator and User guidance. All four models have the same printing speed. The difference between the four models is the package of optional features selected by the consumer (see Table 1). The hardware included in the TOE is shown in Figure 1. While this figure does show the four optional paper trays (bottom) and optional finisher (left side of the photograph), the optional FAX card is an internal component that is not visible.[5]

Figure 1: Xerox WorkCentre 4150 / 4150s / 4150x / 4150xf

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

[5] 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.

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

Table 2: Evaluated Software/Firmware version

Software Item	Optional? (See Table 1)	WorkCentre 4150/4150s/4150x/4150xf
System Software	**No**	**10.100.45.021**
Main Controller	**No**	**1.01.04.35A**
IOT Software	**No**	**1.00.28**
UI	**No**	**0.030.32.004**
Network Controller	**No**	**2.01.56A**
Document Feeder Software	**No**	**1.02**
Finisher Software	**Yes**	**3.06.05**
Tray Firmware	**Yes**	**1.00.00**

The TOE's physical interfaces include a power port, Ethernet port, USB 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)
- Information Flow (TSF_FLOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)

- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Security Management (TSF_FMT)
- TOE Security Architecture (TSF_ARCH)

2.3.1 Image Overwrite (TSF_IOW)

The TOE has an "Image Overwrite" function that overwrites files created during copy (landscape/stapled type only), 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 copy (landscape/stapled type only), 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. FAX jobs are not written to the hard drive and need not to be overwritten.

2.3.2 Information Flow (TSF_FLOW)

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

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

2.3.3 System Authentication (TSF_SYS_AUT)

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

2.3.4 Network Authentication (TSF_NET_AUT)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server (a trusted remote IT entity). The user is not required to login to the network; the account is authenticated by the server

as a valid user. The remote authentication services supported by the TOE are: Kerberos (Solaris), Kerberos (Windows 2000/2003), and SMB (Windows NT.4x/2000/2003).

2.3.5 Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs are available to TOE administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit records; the downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

2.3.6 Cryptographic Operations (TSF_FCS)

The TOE utilizes data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-180, SSLv3.

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

2.3.7 User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing (SSLSec SFP). As provided for in the SSLv3 standard, the TOE will negotiate with the clients to select the encryption standard to be used for the session, to include operating in backward-compatible modes for clients that do not support SSLv3. SSL must be enabled before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option.

2.3.8 User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is generated by the system administrator specifying a series of rules to “accept” packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE WebUI.

2.3.9 Security Management (TSF_FMT)

Only authenticated system administrators can perform the following operations:

- Enable or disable Immediate Image Overwrite;
- Enable or disable On-Demand Image Overwrite;
- Change the system administrator PIN;
- Invoke or Abort (cancel) ODIO;
- Manually invoke “On Demand” Image Overwrite.
- Enable or disable SSL support;
- Create and install X.509 certificates;
- Enable, disable and download the audit log;
- Enable, disable and configure (rules) IP filtering.

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

2.4 TOE Security Architecture (TSF_ARCH)

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

2.5 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. While the TOE will be evaluated with SSL enabled, this security feature should be configured and enabled or disabled in accordance with the consumer’s established security policies. All other configuration parameter values are optional.

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).

A.SANE_NETWORK	All network components connected to the network to which the TOE is connected pass data correctly without modification.
A.SAME_CONTROL	All of the systems that communicate with the TOE are under the same management and physical control as the TOE and are covered by the same management and security policy as the TOE.
A.EXT_RFC_COMPLIANT	All of the remote trusted IT products that communicate with the TOE implement the external half of the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (i.e., SSL) and work as advertised.
A.CHANGE_SA_PIN	System administrators PIN is changed according to the following: 8-digit PIN every 40 days 9-digit PIN every year
A.PROCEDURE	Procedures exist for granting system administrator(s) access to the TSF.

3.2 Threats

3.2.1 Threats Addressed by the TOE

Table 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.[6] This threat only exists if the FAX board is installed and connected to the PSTN.
T.USER	A user, at any time, may attempt to reconfigure the TOE, for the purpose of disabling security functions or intercepting sensitive information or data, either by attempting to access the management functions directly or by logging in as the system administrator.
T.COMM_SEC	An attacker may break into a communications link between the TOE and a remote trusted IT product in order to intercept, and/or modify, information passed to/from/between the TOE and remote trusted IT product.
T.TOE_SEC	An attacker may use the network as a conduit to attempt to break into the TOE WebUI by using vulnerabilities or carefully crafted packets.

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

3.2.2 Threats Addressed by the IT Environment

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

Table 5: Threat Addressed by the IT Environment

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

3.3 Organizational Security Policies

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

Table 6: Organizational Security Policy(s)

Policy	Description
P.COMMS_SEC	TOE supported network security mechanisms (i.e., IP filtering) shall be employed per, and in accordance with, local site security policy.
P.HIPAA_OPT	(Appropriate to organizations under HIPAA oversight) All audit log entries (scan) will be reviewed periodically (the period being local site specific and to be determined by the local audit cyclic period) and in accordance with 45 CFR Subtitle A, Subchapter C, Part 164.530(c),(e),(f) which covers safeguards of information (c), sanctions for those who improperly disclose (e), and mitigation for improper disclosures (f). [7]

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

P.SSL_ENABLED	Secure Socket layer network security mechanisms shall be supported by the TOE and employed as dictated by local site policy.

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

4 SECURITY OBJECTIVES

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

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

4.1 Security Objectives for the TOE

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

The TOE accomplishes the security objectives defined in Table 7.

Table 7: Security Objectives for the TOE

Objectives	Description
O.AUDITS	The TOE must record, protect, and provide to system administrators audit records relative to data scan transmissions through the TOE that (may) have HIPAA-privileged information.
O.RECOVER	Temporary document image data from a copy (landscape/stapled type only), 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. 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.
O.MANAGE	The TOE will provide the functions and facilities necessary to support system administrators responsible for the management of the TOE. The TOE must require that system administrator(s) authenticate with a PIN before allowing access to management functions. The PIN must be obscured as it is entered by the system administrator. The Local UI will be locked until power is cycled once 3 invalid login attempts have been detected. The WebUI will send an error code

	after every invalid authentication attempt.
O.CONTROL_ACCESS	The TOE will provide the system administrator with the ability to determine network access/information flow to and/or from the TOE and to and/or from trusted remote IT products.
O.PROTECTCOM	The TOE must protect user data from disclosure, or modification, by establishing a trusted channel between the TOE and another trusted IT product over which the user data is transported.

4.2 Security Objectives for the Environment

4.2.1 Security objectives for the IT Environment

Table 8: 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 9: 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 according to the configuration under evaluation and will not remove the TOE from its evaluated configuration. Especially Image Overwrite Security accessory is installed and enabled and IIO and ODIO are enabled.
OE.NETWORK_I&A	The TOE environment shall provide, per site specific policy, the correct and accurately functioning Identification and Authentication mechanism(s) that are compatible with, and for external use by, the

Objectives	Description
	TOE.
OE.ACCESS	The TOE will be located in an office environment where it will be monitored by the office personnel for unauthorized physical connections, manipulation or interference.
OE.ADMIN	At least one responsible and trustworthy individual (system administrator) will be assigned, according to onsite procedures for granting access to the PIN, to manage the TOE. The individual(s) have to follow the instructions provided in the administrator and user guidance as well as the security guidance found at http://www.xerox.com/security
OE.PROTECT_COM	The TOE environment must protect user data from disclosure, or modification, by establishing a trusted channel between itself and the TOE over which the data is transported prior to data transmission.

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 copy (landscape/stapled type only), 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 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 2.3.3) restricts the information flow between the PSTN port of the optional FAX board (if installed) and the internal network by implementing a store-and-forward principle.

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

- Only the main controller (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 memory area on the Main Controller board.

- RECEIVING FAX: The Main Controller board must have terminated the PSTN connection before initiating any further processing of FAX data.

- SENDING FAX: The main controller must have finished the copy operation of the fax image to the memory area of the main controller board before opening the PSTN connection 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 main controller works in this situation in a different way.

5.1.3 SSL SFP (TSP_SSL)

The security function "User Data Protection -- SSL" (TSF_FDP_SSL) (see 2.3.7) requires that network traffic to and from the TOE will be encrypted in accordance with the rules defined by the system administrator at the Web User Interface configuration editor for SSL. This policy will be enforced on:

- SUBJECTS: Web clients.

- INFORMATION: All web-based traffic to and from that destination.

- OPERATIONS: HTTP commands.

5.1.4 IP Filter SFP (TSP_FILTER)

The security function "User Data Protection -- IP Filtering" (TSF_FDP_FILTER) (see 2.3.8) requires that network traffic to and from the TOE will be filtered in accordance with the rules defined by the system administrator at the Web User Interface configuration editor for IP Filtering. This policy will be enforced on:

- SUBJECTS: External entities that send network traffic to the TOE.

- INFORMATION: All WebUI-based traffic to and from that destination.
- OPERATIONS: Pass network traffic.

5.1.5 Privileged User Access SFP (TSP_FMT)

The security function "Security Management" (TSF_FMT) (see 2.3.11) restricts management of TOE security functions to the authorized system administrator.

5.2 TOE Security Functional Requirements

5.2.1 Class FAU: Security Audit

5.2.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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

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

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

c. [the events specified in Table 10 below].

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

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

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the events specified in Table 10 below].

Table 10: Audit Events

The audit log will have the following fixed size entries: • Entry number (an integer value from 1 to the number of entries in the audit log) • Event Date (mm/dd/yy) • Event Time (hh:mm:ss)

- Event ID (a unique integer value – see table entries below)
- Event Description (a brief description of an entry that should match the unique Entry ID value – see table entries below)
- Entry Data (This value is any additional data that is logged for an audit log entry – see table entries below)

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

10	Audit Log Disabled	Device name; Device serial number
11	Audit Log Enabled	Device name; Device serial number
12	Print/Fax Driver NOTE: this entry corresponds to LanFax	Job name; User Name; Completion Status; IIO status; Accounting User ID; Accounting Account ID; total-fax-recipient-phone-numbers; fax-recipient-phone-numbers.

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

Dependencies: FPT_STM.1 Reliable time stamp

5.2.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1: The TSF shall provide [system administrator(s)] with the capability to read [all information] from the audit records.

FAU_SAR.1.2: The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

5.2.1.3 FAU_SAR.2 Restricted audit Review

Hierarchical to: No other components.

FAU_SAR.1.1: The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

5.2.1.4 FAU_STG.1 Protected audit trail storage

Hierarchical to: None.

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

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

Dependencies: FAU_GEN.1 Audit data generation

5.2.1.5 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3.

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

Dependencies: FAU_STG.1 Protected audit trail storage

5.2.2 Class FCS: Cryptographic Support

5.2.2.1 FCS_CKM.1 (1) Cryptographic key generation

Hierarchical to: No other components.

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

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

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

5.2.2.2 FCS_CKM.1 (2) Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [OpenSSL RSA key pair generation] and specified cryptographic key sizes [1024 bits or smaller key sizes required for SSLv3 non-capable clients] that meet the following: [not specified].

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

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

5.2.2.3 FCS_CKM.2 (1) Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1(1) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA encrypted exchange of session keys for SSL handshake] that meet the following: [SSLv3 standard].

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

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

5.2.2.4 FCS_CKM.2 (2) Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1(2) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [digital certificates for public RSA keys] that meet the following: [certificate format given in X.509v3].

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

5.2.2.5 FCS_COP.1 (1) Cryptographic operation

Hierarchical to: No other components.

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

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

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

5.2.2.6 FCS_COP.1 (2) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(2) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [RC4, DES or Triple DES] and cryptographic key sizes [56 bit, 128 bit or 168 bit] that

meet the following: [SSLv3 standard – SSL_RSA_WITH_RC4_128_SHA cipher suite].

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

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

5.2.2.7 FCS_COP.1 (3) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(2) The TSF shall perform [secure hashing] in accordance with a specified cryptographic algorithm [MD5 or SHA-1] and cryptographic key sizes [none] that meet the following: [MD5 – RFC 1321 or SHA-1 – FIPS-180].

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

5.2.2.8 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

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

5.2.3 Class FDP: User Data Protection

5.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [Privileged User Access SFP] on [• Subjects: authorized users; • Information: management interfaces; • Operations: access management interfaces].
Dependencies:	FDP_ACF.1 Simple security attributes

5.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [Privileged User Access SFP] to objects based on [• Subjects: Authorized users – role; • Objects: Management interfaces – role].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Authorized user(s) in System Administrator role will be granted access to the TOE management interfaces].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules [no additional access rules].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [no denial of access rules].
Dependencies:	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static attribute initialisation

1

5.2.3.3 FDP_IFC.1 (1) Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1(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

5.2.3.4 FDP_IFF.1 (1) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(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(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- A MFD job of the type copy (landscape/stapled type only), print, network scan or scan to e-mail may store image information in the reserved space on the hard disk drive.

].

FDP_IFF.1.3(1) 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(1) The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5(1) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules: [

- A MFD job of the type 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

5.2.3.5 FDP_IFC.1 (2) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(2) The TSF shall enforce the [Information Flow Control Policy (TSP_FLOW)] on [
subjects: the main controller network port, the FAX board PSTN port
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

5.2.3.6 FDP_IFF.1 (2) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(2) The TSF shall enforce the [Information Flow Control Policy (TSP_FLOW)] based on the following types of subject and information security attributes: [

- the main controller
  - copy operation from/to the memory area of the main controller board in progress or not
- 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 main controller)

].

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- The main controller controls the writing of incoming FAX image and job data to its own memory.
- The main controller controls the reading of outgoing FAX image and job data from its own memory.
- The main controller does not simultaneously activate the network and PSTN ports for the same job.

].

FDP_IFF.1.3(2) The TSF shall enforce [the following additional information flow control SFP rules

- The main controller controls the entire operation of the FAX board via a physical interface.

].

FDP_IFF.1.4(2)	The TSF shall provide the following [no additional SFP capabilities].
FDP_IFF.1.5(2)	The TSF shall explicitly authorise an information flow based on the following rules: [none].
FDP_IFF.1.6(2)	The TSF shall explicitly deny an information flow based on the following rules: [none].
	].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

5.2.3.7 FDP_IFC.1(3) Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1(3)	The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] on [• Subjects: External entities that send traffic to the TOE; • Information: All WebUI-based traffic to/from that destination; • Operations: pass network traffic].
Dependencies:	FDP_IFF.1 Simple security attributes

5.2.3.8 FDP_IFF.1(3) Simple security attributes

Hierarchical to:	No other components.
FDP_IFF.1.1(3)	The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] based on the following types of subject and information security attributes: [• Subjects: Source IP address, • Information: none].
FDP_IFF.1.2(3)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [• The source IP address is in the TOE's rule base
FDP_IFF.1.3(3)	The TSF shall enforce the [implicit allow if no rule is found].
FDP_IFF.1.4(3)	The TSF shall provide the following [none].

FDP_IFF.1.5(3)	The TSF shall explicitly authorize an information flow based on the following rules: [if the rule is the default all].
FDP_IFF.1.6(3)	The TSF shall explicitly deny an information flow based on the following rules: [if there are no rules with matching security attributes].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization.

5.2.3.9 FDP_IFC.1(4) Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1(4)	The TSF shall enforce the [SSLSec SFP (TSP_SSL)] on [• Subjects: Web clients; • Information: All web-based traffic to/from that destination; • Operations: HTTP commands].
Dependencies:	FDP_IFF.1 Simple security attributes

5.2.3.10 FDP_IFF.1(4) Simple security attributes

Hierarchical to:	No other components.
FDP_IFF.1.1(4)	The TSF shall enforce the [SSLSec SFP (TSP_SSL)] based on the following types of subject and information security attributes: [• Subjects: web clients and servers – X.509 certificates; web clients – user role; • Information: none].
FDP_IFF.1.2(4)	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [• SSL session establishment and maintenance are in accordance with the SSLv3 standard. • The SSL cryptographic operations are in accordance with the SSLv3 standard as implemented within the OpenSSL cryptographic libraries. • The signature on any(all) X.509 certificate received by the MFD is valid

- All web-based traffic to and from the remote IT entity shall be over an HTTPS connection]

FDP_IFF.1.3(4)	The TSF shall enforce the [no additional information flow control SFP rules].
FDP_IFF.1.4(4)	The TSF shall provide the following [no additional SFP capabilities].
FDP_IFF.1.5(4)	The TSF shall explicitly authorize an information flow based o the following rules: [no additional rules based on security attributes that explicitly authorize information flows].
FDP_IFF.1.6(4)	The TSF shall explicitly deny any information flow based on the following rules: [not additional rules based on security attributes that explicitly deny information flows].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization

5.2.3.11 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: [copy (landscape/stapled type only), 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.

5.2.3.12 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to:	No other components
FDP_UCT.1.1	The TSF shall enforce the [SSLSec SFP (TSP_SSL)] to be able to *transmit and receive* objects in a manner protected from unauthorized disclosure.
Dependencies:	[FDP_ITC.1 Inter-TSF trusted channel

FTP_TRP.1 Trusted Path]

[FDP_ACC.1 Subset Access Control or

FDP_IFC.1 Subset information flow control]

5.2.3.13 FDP_UIT.1 Data exchange integrity

Hierarchical to:	No other components
FDP_UIT.1.1	The TSF shall enforce the [SSLSec SFP (TSP_SSL)] to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and/or replay*.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.2.4 Class FIA: Identification and Authentication

5.2.4.1 FIA_AFL.1 (1) Authentication failure handling

Hierarchical to:	No other components
FIA_AFL.1.1(1)	The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [authentication at the local user interface].
FIA_AFL.1.2(1)	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lockout the SA login until the power has been cycled].
Dependencies:	FIA_UAU.1 Timing of authentication

5.2.4.2 FIA_AFL.1 (2) Authentication failure handling

Hierarchical to:	No other components
FIA_AFL.1.1(2)	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(2)	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [send the "403 Authorization Required" HTTP error code to this Browser session].
Dependencies:	FIA_UAU.1 Timing of authentication

Application Note: While the "403 Authorization Required" code is sent by the TOE to the browser in accordance with the HTTP protocol standard, each individual browser may display the code to the user differently. Some may display the error code, some may display a "user friendly" message and still others may simply re-prompt for correct authentication credentials.

5.2.4.3 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

5.2.4.4 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

5.2.4.5 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 user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.2.5 Class FMT: Security Management

5.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components

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

- TSF_IOW
- TSF_NET_AUT
- TSF_FAU
- TSF_FDP_SSL
- TSF_FDP_FILTER

to [the system administrator].

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

5.2.5.2 FMT_MTD.1(1) Management of TSF data

Hierarchical to: No other components

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

- Audit log]

to [the system administrator].

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

5.2.5.3 FMT_MTD.1(2) Management of TSF data

Hierarchical to: No other components

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

- X.509 Server certificate]

to [the system administrator].

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

5.2.5.4 FMT_MTD.1(3) Management of TSF data

Hierarchical to: No other components

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

- IP filter rules]

to [the system administrator].

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

5.2.5.5 FMT_MSA.1 (1) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(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

5.2.5.6 FMT_MSA.3 (1) Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1(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(1)	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.

5.2.5.7 FMT_MSA.1 (2) Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1(2)	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

5.2.5.8 FMT_MSA.3 (2) Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1(2)	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(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.

5.2.5.9 FMT_MSA.1 (3) Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1(3)	The TSF shall enforce the [SSL SFP (TSP_SSL)] to restrict the ability to *[enable or disable]* the security attributes [SSL] to [the system administrator].
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

5.2.5.10 FMT_MSA.3 (3) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(3) The TSF shall enforce the [SSL SFP (TSP_SSL)] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) 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 (3) and FMT_MSA.3 (3) apply to the SSL function. The only configuration option available for SSL is the ability to enable or disable it. While the system administrator can enable or disable SSL, doing so does not change or override default or initial values associated with object creation.

5.2.5.11 FMT_MSA.1 (4) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(2) The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] to restrict the ability to *query, modify, delete* the security attributes [source address] to [they system administrator].

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

5.2.5.12 FMT_MSA.3 (4) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(4) The TSF shall enforce the [IP Filter SFP (TSP_FILTER)] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(4) 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 (4) and FMT_MSA.3 (4) apply to the IP Filter function. The default configuration is permissive (all hosts can connect to the TOE). While the system administrator can configure a restrictive list of hosts that can connect to the TOE (with those hosts not listed unable to connect to the TOE), entering a source address into the list does not change or override default or initial values associated with object creation.

5.2.5.13 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

- Enable/disable Immediate Image Overwrite (IIO);
- Change PIN;
- Invoke/Abort ODIO;
- Enable/disable audit function;
- Transfer the audit records (if audit is enabled) to a remote trusted IT product;
- Enable/disable SSL;
- Create/upload/download X.509 certificates;
- Enable/disable and configure (specify the IP address and/or IP address range for remote trusted IT products (presumed)

allowed to connect to the TOE via the network interface) IP filtering].

Dependencies: No Dependencies

5.2.5.14 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

5.2.6 Class FPT: Protection of the TSF

5.2.6.1 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No Dependencies

5.2.6.2 FPT_SEP.1 Domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No Dependencies

5.2.6.3 FPT_STM.1 Reliable time stamp

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

5.2.7 Class FTP: Trusted path/channels

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *the TSF* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [transmission of network scan data to the scan repository].
Dependencies:	No dependencies

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

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication channel between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2	The TSF shall permit [*remote*] users to initiate communication via the trusted path.
FTP_ITC.1.3	The TSF shall require use of the trusted path for [• *Print jobs and LanFax jobs submitted via Web UI,* • *the security management functions available to the system administrator from the Web UI*].
Dependencies:	No dependencies

5.3 TOE Security Assurance Requirements

Table 11 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL3, augmented with ALC_FLR3. The SARs are not iterated or refined from Part 3.

Table 11: EAL3 (augmented with ALC_FLR.3) Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.3	Authorisation controls	ALC_DVS.1
ACM_SCP.1	TOE CM coverage	ACM_CAP.3
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.2	Security-enforcing 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_DVS.1	Identification of security measures	
ALC_FLR.3	Systematic flaw remediation	None
ATE_COV.2	Analysis of coverage	ADV_FSP.1
		ATE_FUN.1
ATE_DPT.1	Testing: High-level design	ADV_HLD.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_MSU.1	Examination of guidance	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.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 10^4 – 10^{12} (4 – 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 10^8 to 10^{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)
- Information Flow (TSF_FLOW)
- System Authentication (TSF_SYS_AUT)
- Network Authentication (TSF_NET_AUT)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- Security Management (TSF_FMT)
- TOE Security Architecture (TSF_ARCH)

6.1.1 Image Overwrite (TSF_IOW)

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

The main controller spools and processes documents to be copied (landscape/stapled type only), printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive of the main controller. The definition of this reserved section is statically stored within the TOE and cannot be manipulated. Immediately after the job has completed, the files are overwritten using a three pass overwrite procedure as described in DoD 5200.28-M. FAX jobs do not get written to the HDD.

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

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. Before pressing the abort button,

authentication as system administrator is required. If the System Administrator cancels ODIO at the Local UI, 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. The ODIO cannot be aborted from the Web Interface.

If the TOE is turned back on after a power failure, the TOE automatically alerts the administrator (via a LocalUI notification) that IIO has failed and that an ODIO should be run in order to overwrite all abnormally terminated print or scan jobs prior to coming back "on line".

6.1.2 Information Flow (TSF_FLOW)

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

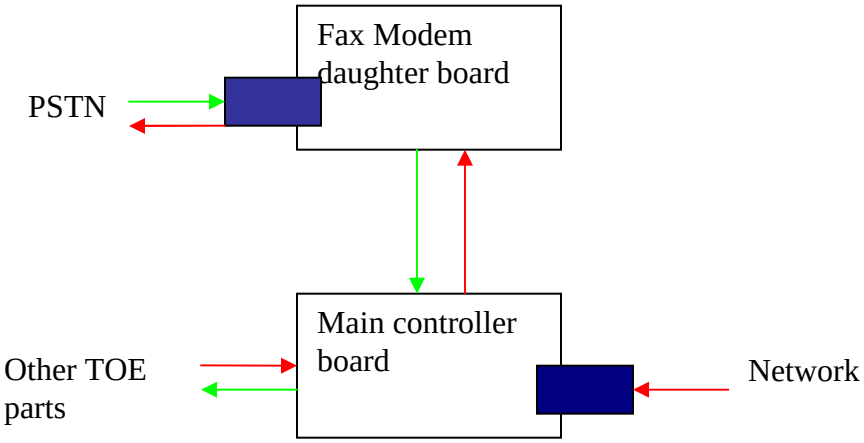

Figure 2: TSF_FLOW

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

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

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

6.1.3 Authentication (TSF_SYS_AUT)

The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions (see 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 will be delayed at the Local User Interface until the power is cycled if 3 wrong PINs were entered in succession. If 1 wrong PIN is entered at the web interface from one particular Browser session, the TOE will send an error message (“HTTP 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 Network Authentication (TSF_NET_AUT)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password which is then validated by the designated authentication server (a trusted remote IT

entity). The user is not required to login to the network; the account is authenticated by the server as a valid user. The remote authentication services supported by the TOE are: Kerberos (Solaris), Kerberos (Windows 2000/2003), and SMB (Windows NT.4x/2000/2003).

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

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

6.1.5 Security Audit (TSF_FAU)

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

The audit log tracks system start-up/shutdown, ODIO start/completion, and print, scan, email, local fax, I-Fax (not evaluated), and LanFax jobs. Copy jobs are not tracked. By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for transmission of data outside of the local environment, as required by such legislation as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc.

The Web UI presents the only access to the audit log; the audit log is not viewable from the local UI. The Web UI screen contains a button labeled “Save as Text File” that is viewable by all users. If this button is selected, and the system administrator is not already logged in through the interface, then a system administrator login alert window is presented. Once the system administrator has successfully logged in, then the audit log file becomes downloadable.

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

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

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

For network scan, email, and IFax (not included in the evaluation) jobs the accounting IDs (i.e., PINS) required by the *XSA*, or *Network Accounting*, will be recorded in the audit log.

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

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

6.1.6 Cryptographic Support (TSF_FCS)

The TOE utilizes data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-180, SSLv3.

6.1.7 User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing. As provided for in the SSLv3 standard, the TOE will negotiate with the clients to select the encryption standard to be used for the session, to include operating in backward-compatible modes for clients that do not support SSLv3. SSL must be enabled before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. The TOE creates and enforces the informal security policy model, “All communications to the Web server will utilize SSL (HTTPS).”

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

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

Additionally, the TOE can act as a web client in the case of Network scanning. When acting as an SSL client to SSL scan repository, the TOE does not validate the remote server’s certificate against a trusted CA.

6.1.8 User Data Protection – IP Filtering (TSF_FDP_FILTER)

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

6.1.9 Security Management (TSF_FMT)

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

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

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

6.1.10 TOE Security Architecture (TSF_ARCH)

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

6.2 Assurance Measures

The TOE satisfies CC EAL3 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 EAL3, augmented with ALC_FLR.3, assurance requirements.

Table 12: Assurance Measures

Assurance Component	How requirement will be met
ACM_CAP.3 Authorisation Controls	The vendor provides configuration management documents and a Configuration Item list.
ACM_SCP.1 TOE CM coverage	The vendor provides a Configuration Item list that includes the evaluation evidence.
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.2 Security enforcing 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_DVS.1 Identification of security measures	The vendor submits their developmental security procedures.
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.2 Analysis of coverage	The analysis of test coverage is submitted in the evaluation evidence.
ATE_DPT.1 Testing: High-level design	The depth of testing analysis is submitted in the evaluation evidence.
ATE_FUN.1 Functional testing	The test evidence is submitted to the CCTL.
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_MSU.1 Examination of guidance	The laboratory analyses the submitted Security Target, User and Administrator guidance, Development documentation and testing evidence.
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 , identified threats to be countered or organizational security policies.

Table 13: Security Objectives Rationale (Threats)

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. 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.
T.TOE_SEC	O.CONTROL_ACCESS	O.CONTROL_ACCESS helps mitigate the threat T.TOE_SEC by ensuring that the administrator has the ability to control network access and information flow to the WebUI by implementing IP Filter in order to determine which network resources are allowed to connect to the WebUI which will limit an attacker's access to the TOE.

Threat	Objective	Rationale
T.COMM_SEC	O.PROTECTCOM	O.PROTECTCOM helps mitigate the threat T.COMM_SEC by ensuring that a fully-compliant trusted channel between the TOE and another remote trusted IT product exists to protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
TE.COMM_SEC	OE.PROTECT_COM	OE.PROTECT_COM helps mitigate the threat TE.COMM_SEC by ensuring that a trusted communication channel between the TOE and remote trusted IT products is established to protect user data from disclosure or modification.

Table 14: Security Objectives Rationale (Assumptions and OSPs)

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

Assumption / Threat	Objective	Rationale
		OE.INSTALL covers the remaining part of A.NO_EVIL_ADM because the objective ensures that the system administrator configures the TOE according to the configuration under evaluation and will not remove the TOE from its evaluated configuration (especially that the Image Overwrite Security accessory is installed and enabled).
A.NETWORK	OE.NETWORK	OE.NETWORK covers A.NETWORK by requiring a mechanism to detect network-based attacks against the TOE.
A.SAME_CONTROL	OE_NETWORK_I&A	OE.NETWORK_I&A supports the assumption A.SAME_CONTROL by ensuring the presence within the environment of a fully-functioning I&A mechanism to limit the ability of an attacker to intercept communications between the TOE and a remote trusted IT product and to ensure that such remote products are under the same management and subject to the same security policy as the TOE.
A.EXT_RFC_COMPLIANT	OE.PROTECT_COM	A.EXT_RFC_COMPLIANT ensures a trusted channel between the TOE and another remote trusted IT product exists to protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
A.CHANGE_SA_PIN	OE.ADMIN	OE.ADMIN covers parts of A.CHANGE_SA_PIN because "*responsible and trustworthy individuals*" are "*not careless, willfully negligent or hostile*". Furthermore, the individuals have to follow the instructions provided in the guidance documents, including those that prescribe guidance for composition of the TOE SA PIN.
A.PROCEDURE	OE.ADMIN	OE.ADMIN covers A.PROCEDURE by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE.
P.HIPAA_OPT	O.AUDITS	O.AUDITS helps satisfy OSP P.HIPAA_OPT by ensuring that log entries are provided by the TOE for periodic review by system administrators, in order to ensure that safeguards for information mandated by applicable laws and regulations remain in place, and that audit logs available to mitigate the risk of improper disclosure and to support application of sanctions following improper disclosure.
P.COMM_SEC P.SSL_ENABLED A.EXT_RFC_COMPLIANT	O.PROTECTCOM	O. PROTECTCOM helps meet OSPs P.COMMS_SEC and P.SSL_ENABLED by ensuring that fully-compliant (A.EXT_RFC_COMPLIANT) trusted channel between the TOE and another remote trusted IT product exists to

Assumption / Threat	Objective	Rationale
		protect user data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product.
P.COMMS_SEC P.SSL_ENABLED	OE.PROTECT_COM	OE.PROTECT_COM meet the OSPs P.COMMS_SEC AND P.SSL_ENABLED by ensuring that a trusted communication channel between the TOE and remote trusted IT products is established to protect user data from disclosure or modification.

8.2 Security Requirements Rationale

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

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

8.2.1 Rationale For TOE Security Requirements

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

Table 15: 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 restricts the access to this function to the system administrator. FMT_SMR.1 manages the role “system administrator”. FMT_SMR.1 ensures that the TOE maintains the system

Objective	Rationale
	administrator role – a trusted individual who can administer the TOE. 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 Fax jobs will not be written to the HDD at all. FDP_IFF.1(3) - (6), FDP_IFC.1(3) - (6), FDP_UCT.1 and FDP_UIT.1 ensure that the IP_Filter SFP, and SSL_SFP are enforced to control and protect information flow between controlled subjects (IP address) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner and the protection and removal of residual user data from a controlled resource.
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. 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	FAU_GEN.1 ensures that the TOE is able to generate time-stamped audit records of a specified set of security-relevant events related to TOE operations. FAU_SAR.1 and FAU_SAR.2 ensure that the TOE is able to make available only to users granted explicit “read” access (TOE administrators) audit information in a form suitable for viewing and evaluation/analysis. FIA_AFL.1 (1) ensures that the TOE takes specific and immediate self-protection action when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Local User Interface. FIA_AFL.1 (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

Objective	Rationale
	the properties of a web interface (no dependable identification of the user's terminal and therefore no possibility to lock this terminal) FIA_UAU.2 and FIA_UID.2 ensure that system administrators are authenticated (and implicitly identified) before accessing the security functionality of the TOE. FIA_UAU.7 ensures that only obscured feedback generated by the authentication process is provided to system administrators before successful authentication. FIA_UID.2 ensures that the System Administrator and other users aresuccessfully identified. FMT_MOF.1 restricts the access to these management functions to the system administrator. FMT_MTD.1 (2) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to create or delete the X.509 Server certificate. FMT_SMF.1 ensures that the security management functions (i.e., enable/disable IIO and ODIO, change system administrator PIN, and invoke/abort ODIO) are available on the TOE. FMT_SMR.1 manages the role "system administrator". FPT_RVM.1 ensures that TOE security policy enforcement functions are invoked and successful before any TOE function is allowed to proceed. FTP_ITC.1 and FTP_TRP.1 ensure that the TOE provides communications channels between itself and remote trusted IT products and remote users distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
O.AUDITS	FAU_GEN.1 ensures that the TOE is able to generate time-stamped audit records of a specified set of security-relevant events related to TOE operations. FAU_SAR.1 and FAU_SAR.2 ensure that the TOE is able to make available only to users granted explicit "read" access (TOE administrators) audit information in a form suitable for viewing and evaluation/analysis. FAU_STG.1 and FAU_STG.4 ensure that the TOE is able to prevent unauthorized modification of audit trail records and,

Objective	Rationale
	when the audit trail file is full, is able to overwrite the oldest stored audit records without other modification to stored records. FMT_MTD.1 (1) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to clear, delete, create, read and download the audit log. FPT_STM.1 ensures that the TOE provides a reliable timestamp for inclusion in the audit log.
O.CONTROL_ACCESS	FDP_IFF.1(3) - (6), FDP_IFC.1(3) - (6), FDP_UCT.1 and FDP_UIT.1 ensure that the IP_Filter SFP is enforced to control and protect information flow between controlled subjects (IP address) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner. FMT_MTD.1 (3) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to and query, modify, delete or create the IP filter rules. FPT_SEP.1 ensures that the TOE maintains a security domain for its own use to protect against interference or tampering by untrusted subjects. FMT_MSA.3 (4) and FMT_MSA.1 (4) define the possible actions that a system administrator can take concerning IP Filter.
O.PROTECTCOM	FCS_CKM.1 (1 – 2), FCS_CKM.2 (1 – 2), FCS_CKM.4 and FCS_COP.1 (1 – 3) ensure that the TOE provides the cryptographic support and services, secure hashing and associated key management capabilities necessary to assure secure communication between TOE components and remote trusted products by using specified cryptographic key generation algorithms and associated cryptographic key distribution and destruction methods. FDP_ACC.1 and FDP_ACF.1 ensure that the TOE enforces the PrivUserAccess SFP on subjects, objects, information, and operations and applies specific rules on all operations involving controlled subjects and objects, limiting access to management

Objective	Rationale
	interfaces to the System Administrator. FDP_IFF.1(3) - (6), FDP_IFC.1(3) - (6), FDP_UCT.1 and FDP_UIT.1 ensure that the IP_Filter SFP, and SSL_SFP are enforced to control and protect information flow between controlled subjects (IP address) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner and the protection and removal of residual user data from a controlled resource. FMT_MTD.1 (2) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to create or delete X.509 Server certificates. 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. FPT_RVM.1 ensures that TOE security policy enforcement functions are invoked and successful before any TOE function is allowed to proceed. FMT_MSA.3 (3) and FMT_MSA.1 (3) define the possible actions that a system administrator can take concerning SSL.

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 3 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 16 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 16: 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 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_SYS_AUT	FIA_UAU.2	TSF_SYS_AUT ensures that system administrators must authenticate before accessing the security functionality of the TOE.
	FIA_UID.2	TSF_SYS_AUT ensures that the system administrators must be identified (to include the

TSF	SFR	Rational
		implicit identification when the "Tools" menu is entered at the Local User Interface) before accessing the security functionality of the TOE.
	FIA_UAU.7	TSF_SYS_AUT ensures that only obscured feedback is generated by the authentication process.
	FIA_AFL.1 (1)	TSF_SYS_AUT ensures that the TOE locks the Local User Interface until the power is cycled if three unsuccessful authentication attempts happened at this user interface.
	FIA_AFL.1 (2)	TSF_SYS_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_SYS_AUT only knows the role "system administrator".
TSF_NET_AUT	FIA_UID.2	Users must be identified before being permitted to use TOE network resources.
	FIA_UAU.2	TSF_NET_AUT ensures that users must authenticate (via third party methods such as Kerberos or LDAP) before accessing the network resources of the TOE.
	FIA_UAU.7	TSF_NET_AUT ensures that only obscured feedback is generated by the authentication process.
	FAU_GEN.1	TSF_NET_AUT uses the authenticated user name as part of the job context in the system audit log.
TSF_FAU	FAU_GEN.1	TSF_FAU ensures that the TOE generates audit logs of system and user actions/events.
	FAU_SAR.1	TSF_FAU ensures that the system administrator has the capability to review the audit logs.
	FAU_SAR.2	TSF_FAU ensures that the capability of reviewing the audit logs is restricted to the system administrator.
	FAU_STG.1	TSF_FAU ensures that the audit logs cannot be deleted or modified.
	FAU_STG.4	TSF_FAU ensures that the audit log will not fill up so that events are not recorded.
	FPT_STM.1	TSF_FAU ensures that the TOE will have access to a reliable timestamp for marking audit records.

TSF	SFR	Rational
	FIA_UID.2 FIA_UAU.2	TSF_FAU ensures that user identities can be associated with their actions as recorded in the audit logs.
	FIA_AFL.1 (2)	TSF_FAU requires that the system administrator authenticate prior to viewing the audit logs.
TSF_FCS	FCS_CKM.1 (1 - 2)	TSF_FCS ensures that the TOE generates cryptographic keys as defined in the SSL v3 standard with key sizes of 128-bit (RC4), 56-bit (DES) and 168-bit (Triple DES) that meet the generation and exchange of session keys a defined in the SSL v3 standard with the cipher suites defined in FCS_COP.1 (2). TSF_FCS ensures that the TOE generates cryptographic keys in accordance with OpenSSL RSA key pair generation with key sizes of 1024 bits. TSF_FCS ensures that the TOE generates cryptographic keys in accordance with Triple Data Encryption Standard (3DES-EDE) with key sizes of 3 unique 56-bit keys that meets FIPS-42-2, FIPS-74, FIPS-81.
	FCS_CKM.2 (1 - 2)	TSF_FCS ensures that the TOE distributes cryptographic keys in accordance with RSA encrypted exchange of session keys for SSL handshake that meets the SSLv3 standard. TSF_FCS ensures that the TOE distributes cryptographic keys in accordance with digital certificates for public RSA keys that meets the certificate format given in X.509v3.
	FCS_CKM.4	TSF_FCS ensures that the TOE destroys cryptographic keys in accordance with semiconductor memory state loss at power-down, semiconductor memory zeroization at power-up.
	FCS_COP.1 (1 - 3)	TSF_FCS ensures that the TOE performs digital signature generation and verification in accordance with RSA (1024 bits) that meets the SSLv3 standard. TSF_FCS ensures that the TOE performs encryption and decryption in accordance with RC4 (128 bit), DES (56 bit) and Triple DES (168-bit) that meet SSLv3 standard – SSL RSA WITH RC4 128 SHA cipher suite. TSF_FCS ensures that the TOE performs cryptographic checksum generation and secure hash (message digest) computation in

TSF	SFR	Rational
		accordance with MD5 that meets RFC1321. TSF_FCS ensures that the TOE performs cryptographic checksum generation and secure hash (message digest) computation in accordance with SHA-1 that meets FIPS-180.
TSF_FDP_SSL	FCS_CKM.1 (1)	TSF_FDP_SSL ensures that the TOE generates cryptographic keys as defined in the SSL v3 standard with key sizes of 128-bit (RC4) that meets the generation and exchange of session keys a defined in the SSL v3 standard with the cipher suites defined in FCS_COP.1 (2).
	FCS_CKM.1 (2)	TSF_FDP_SSL ensures that the TOE generates cryptographic keys in accordance with OpenSSL RSA key pair generation with key sizes of 1024 bits.
	FCS_CKM.2 (1)	TSF_FDP_SSL ensures that the TOE distributes cryptographic keys in accordance with RSA encrypted exchange of session keys for SSL handshake that meets the SSLv3 standard.
	FCS_CKM.2 (2)	TSF_FDP_SSL ensures that the TOE distributes cryptographic keys in accordance with digital certificates for public RSA keys that meets the certificate format given in X.509v3.
	FCS_COP.1 (1)	TSF_FDP_SSL ensures that the TOE performs digital signature generation and verification in accordance with RSA (1024 bits) that meets the SSLv3 standard.
	FDP_IFC.1 (4)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP on Web clients; all web-based traffic to/from that destination; HTTP commands.
	FDP_IFF.1 (4)	TSF_FDP_SSL ensures that the TOE enforces the SSLSec SFP based on web clients and servers – X.509 certificates and based on web clients user roles. TSF_FDP_SSL ensures that the TOE permits an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: SSL session establishment and maintenance are in accordance with the SSLv3 standard; the SSL cryptographic operations are in accordance with the SSLv3 standard as implemented within the OpenSSL cryptographic libraries; the signature on any(all) X.509 certificate received by

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

TSF	SFR	Rational
		controlled information via a controlled operation if the following rules hold: the source IP address is in the TOE's rule base. TSF_FDP_FILTER ensures that the TOE enforces the implicit allow if no rule is found, explicitly authorizes an information flow if the rule is the default all, and explicitly denies an information flow if there are no rules with matching security attributes.
	FMT_MSA.3 (4) FMT_MSA.1 (4)	The IPFilter parameters (address, protocol, port) can be defined by the system administrator.
TSF_FMT	FDP_ACC.1 FDP_ACF.1	TSF_FMT ensures that the TOE will restrict access to management interfaces and objects to the system administrator.
	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.
	FMT_SMR.1	TSF_FMT ensures that the TOE maintains a security administrator role and can associate a human user with that role.
	FMT_MTD.1 (1) FMT_MTD.1 (2) FMT_MTD.1 (3)	TSF_FMT ensures that the ability to modify certain TSF data is restricted to the system administrator.
TSF_ARCH	FPT_RVM.1 FPT_SEP.1	While not a TSF in the classic sense of the term, the functionality that would be associated with TSF_ARCH is present and represented by the security functional requirements (SFRs) FPT_RVM.1 and FPT_SEP.1 based strictly on the TOE definition and architecture.

8.5 TOE Assurance Requirements

Section 6.2 of this document identifies the Assurance Measures implemented by Xerox to satisfy the assurance requirements of EAL3, augmented with ALC_FLR.3, as delineated in the table in Annex B of the CC, Part 3. Table 17 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.3.

Table 17: Assurance Measure Compliance Matrix

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

FIA_UAU.2 / TSF_SYS_AUT: This PIN space (10^8 to 10^{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 18 is a cross-reference of the functional components, their related dependencies, and whether the dependencies are satisfied.

Table 18: SFR Dependencies Status

Functional Component ID	Dependency (ies)	Satisfied
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_CKM.1 (1)	FCS_CKM.2	Yes, FCS_CKM.2 (1)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_CKM.1(2)	FCS_CKM.2	Yes, FCS_CKM.2 (1)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of

Functional Component ID	Dependency (ies)	Satisfied
		attributes (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_CKM.2 (1)	FCS_CKM.1	Yes, FCS_CKM.1 (1)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_CKM.2 (2)	FCS_CKM.1	Yes, FCS_CKM.2 (2)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_COP.1 (1)	FCS_CKM.1	Yes, FCS_CKM.1 (1)

Functional Component ID	Dependency (ies)	Satisfied
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_COP.1 (2)	FCS_CKM.1	Yes, FCS_CKM.1 (2)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_COP.1 (3)	FCS_CKM.1	Yes, FCS_CKM.1 (1), FCS_CKM.1(2)
	FCS_CKM.4	Yes
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (secure hashing), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further,

Functional Component ID	Dependency (ies)	Satisfied
		because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FCS_CKM.4	FCS_CKM.1	Yes, FCS_CKM.1 (1, 2, 3, 4)
	FMT_MSA.2	No. FMT_MSA.2 deals not with the security/correctness of the *functionality* (key generation, key destruction), but with that of *attributes* (key size, algorithm, etc) that are accepted by the TSF. Because the TSF does not merely accept them, but actually supplies them to itself, they must, by definition be secure. The TOE is programmed with these values, and there is no way for the system administrator to modify or delete them, much less in a manner that would compromise the security of the TOE. Further, because the values are programmed into the TOE and are unchangeable, there would be no way to test the FMT_MSA.2 requirement.
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	Yes, FMT_MSA.3 (1, 2, 3, 4)
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_IFC.1 (3)	FDP_IFF.1	Yes, FDP_IFF.1 (3)
FDP_IFF.1 (3)	FDP_IFC.1	Yes, FDP_IFC.1 (3)
	FMT_MSA.3	Yes, FMT_MSA.3 (3)
FDP_IFC.1 (4)	FDP_IFF.1	Yes, FDP_IFF.1 (4)
FDP_IFF.1 (4)	FDP_IFC.1	Yes, FDP_IFC.1 (4)
	FMT_MSA.3	Yes, FMT_MSA.3 (4)
FDP_RIP.1	None	
FDP_UCT.1	FDP_ACC.1	Yes
	FDP_TRP.1	Yes, FDP_TRP.1
FDP_UIT.1	FDP_ACC.1	Yes
	FDP_TRP.1	Yes, FDP_TRP.1
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_UAU.2	FIA_UID.1	Yes, hierarchically by FIA_UID.2. Identification of the system administrator at the Local User Interface

Functional Component ID	Dependency (ies)	Satisfied
		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
FIA_UID.2	None	
FMT_MOF.1	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (1)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (2)	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MTD.1 (3)	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.
	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_MSA.1 (3)	FMT_ACC.1 or	Yes, FDP_IFC.1 (4)

Functional Component ID	Dependency (ies)	Satisfied
	FDP_IFC.1	
	FMT_SMR.1	Yes, FMT_SMR.1
	FMT_SMF.1	Yes, FMT_SMR.1
FMT_MSA.3 (3)	FMT_MSA.1	Yes, FMT_MSA.1 (3)
	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 (4)	FMT_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1 (3)
	FMT_SMR.1	Yes, FMT_SMR.1
	FMT_SMF.1	Yes, FMT_SMR.1
FMT_MSA.3 (4)	FMT_MSA.1	Yes, FMT_MSA.1 (4)
	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.
FTP_RVM.1	None	
FPT_SEP.1	None	
FPT_STM.1	None	
FTP_ITC.1	None	
FTP_TRP.1	None	

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

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

Assurance Component ID	Dependencies	Satisfied
ACM_CAP.3	ALC_DVS.1	Yes
ACM_SCP.1	ACM_CAP.3	Yes
ADO_DEL.1	None	
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.2	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_DVS.1	None	
ALC_FLR.3	None	
ATE_COV.2	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 EAL3 augmented with ALC_FLR.3. The EAL3 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 EAL3.

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 18 and Table 19 and described in Section 8.7.

- The security function 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_SYS_AUT prevent this. If TSF_IOW is activated, bypassing or tampering is not possible.

- TSF_FMT, TSF_NET_AUT, TSF_FAU, TSF_FCS, TSF_FDP_SSL, and TSF_FDP_FILTER provide some security functions and TSF_SYS_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.