# Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target Version 1.0

Prepared by:


Xerox Corporation
1350 Jefferson Road
Rochester, New York 14623

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076


Document Version: 1.0 (April 2009).

# Table of Contents

# List of Figures



# List of Tables

# 1. SECURITY TARGET INTRODUCTION

This Chapter presents Security Target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 11.

## 1.1. ST and TOE Identification

This section provides information needed to identify and control this ST and its associated TOE. This ST targets Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.3.

| | |
|---|---|
| **ST Title:** | Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target |
| **ST Version:** | 1.0 |
| **Revision Number:** | Revision 1.21 |
| **Publication Date:** | April 08, 2009 |
| **Authors:** | Computer Sciences Corporation (US) Common Criteria Testing Laboratory, Xerox Corporation |
| **TOE Identification:** | Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems (see Section 1.3.1 for software version numbers) |

**ST Evaluator:** Computer Sciences Corporation (CSC)

**Keywords:** Xerox, Multi Function Device, Image Overwrite, WorkCentre

# 1.2. TOE Overview

## 1.2.1. Usage and Major Security Features

The product is a multi-function device (MFD) that copies and prints, with scan-to-email, network scan (including "scan to mailbox"), and FAX options. A standard component of the TOE is the Image Overwrite Security package. This function forces any temporary image files created during a print, network scan, scan to email, or LanFax job to be overwritten when those files are no longer needed.

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

**Table 1: Models and capabilities**

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

| | Print | Copy[1] | Network Scan | Embedded Fax[1] | Scan 2 email | Print Speed |
|---|---|---|---|---|---|---|
| WorkCentre 5632 | x | x | o | o | o | Up to 32 ppm |
| WorkCentre 5638 | x | x | o | o | o | Up to 38 ppm |
| WorkCentre 5645 | x | x | o | o | o | Up to 45 ppm |
| WorkCentre 5655 | x | x | o | o | o | Up to 55 ppm |
| WorkCentre 5665 | x | x | o | o | o | Up to 65 ppm |
| WorkCentre 5675 | x | x | o | o | o | Up to 75 ppm |
| WorkCentre 5687 | x | x | o | o | o | Up to 87 ppm |

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

An optional Finisher, which is not part of the TOE, provides "after print" services such as document collation and stapling. The hardware included in the TOE is shown in Figure 1. This figure also shows an optional Finisher connected to the TOE at the right side of the picture and an optional Paper Feeder at the left side of the picture, neither of which are part of the TOE.

**Figure 1: Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687**

*** Also shown are an optional Paper Feeder (left) and Finisher (right).**

The MFD stores temporary image data created during a print, network scan or scan to email, and LanFAX job on an internal hard disk drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The encryption key is created dynamically on each power-up.

Copy jobs are not written to the hard drive and need not to be overwritten. Copy/Print, Store and Reprint jobs are written to the hard drive so that they may be reprinted at a later time; therefore, they will be overwritten when a full on-demand image overwrite is performed. Embedded FAX jobs are written to flash memory and are overwritten at the completion of each job, or on demand of the MFD system administrator.

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

The optional Xerox Embedded Fax accessory provides local analog FAX capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax jobs, if purchased by the consumer. A separate non-volatile memory resource is dedicated to embedded fax, and the image files written to this memory are zeroized at the completion of a fax job.

User image files associated with the Copy/Print, Store and Reprint feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job using the 5200.28-M algorithm. The

stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite.

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

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

The TOE implements lpr/lpd, Port 9100, and SNMP over IPv6.

The TOE provides for user identification and authorization based on either local or remote ACL's as configured by the system administrator.

### 1.2.2. TOE Type

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

### 1.2.3. Required Non-TOE Hardware, Software and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function device, however, the network security features are only useful in environments where the TOE is connected to a network. TSF_NET_ID is only available when remote authentication services (LDAP, NDS, Kerberos, SMB) are present on the network that the TOE is connected to.

## 1.3. TOE Description

This section provides context for the TOE evaluation by identifying the logical and physical scope of the TOE, as well as its evaluated configuration.

### 1.3.1. Physical Scope of the TOE

The TOE is a Multi-Function Device (Xerox WorkCentre model 5632, 5638, 5645, 5655, 5665, 5675, or 5687) that consists of a printer, copier, scanner, FAX (when purchased by the consumer), and email as well as all Administrator and User guidance. The difference between the seven models is their printing speed. The hardware included in the TOE is shown in Figure 1. This figure also shows an optional Finisher connected to the TOE at the right side of the picture and an optional Paper Feeder at the left side of the picture, neither of which are part of the TOE. The optional FAX card is not shown in this figure[1].

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

| Software/Firmware Item | Software/Firmware Version |
|---|---|
| System Software | **21.113.02.000** |
| Network Controller Software | **050.60.50812.P33v1** |
| UI Software | **020.11.030** |
| IOT Software | **91.02.65** |
| SIP Software | **20.11.30** |
| DADH Software (Options) | |
| • Normal Mode | **16.28.00** |
| • Quiet Mode | **25.18.00** |
| FAX Software | **02.28.033** |
| Finisher Software (Options) | |
| • 1K LCSS | **01.27.00** |
| • 2K LCSS | **03.40.00** |
| • HCSS | **13.40.00** |
| • HCSS with BookletMaker | **24.16.00** |
| • High Volume Finisher (HVF) | **04.03.51** |
| • HVF with BookletMaker | **03.06.06** |
| Scanner Software (Options) | |
| • 5632/5655/5665/ | **04.22.00** |

[1] 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.

| Software/Firmware Item | Software/Firmware Version |
|---|---|
| 5675/5687 Models | |
| • 5638/5645 Models | **17.05.00** |

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 above.

**Table 3: System User and Administrator Guidance**

| Title | Version | Date |
|---|---|---|
| System Administration CD1 | 538E11430 | June 12th, 2007 |
| Xerox IUG CD 2 | 538e11441 | September 14th, 2007 |
| Secure Installation and Operation of Your WorkCentre 5632/5638/5645/ 5655/5665/5675/5687 | 1.4 | March 20, 2009 |
| WorkCentre 5632/5638/5645/5655/5665/5675/5687 Quick Use Guide | 604P19210 | --- |

The Administrator and User guidance included in the TOE are listed in Table 3. A system administrator or user can ensure that they have the appropriate guidance by comparing the software version number, displayed when the CD is initially run, to the version numbers listed in the table above.

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

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

### 1.3.2. Logical Scope of the TOE

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

The following security functions are controlled by the TOE:

- Image Overwrite (TSF_IOW)
- Authentication (TSF_ AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU).
- Cryptographic Operations (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSec)
- Network Management Security (TSF_NET_MGMT)
- Information Flow Security (TSF_ FLOW)
- Security Management (TSF_FMT)
- User Data Protection - AES (TSF_EXP_UDE)

#### 1.3.2.1. Image Overwrite (TSF_IOW)

The TOE has an "Image Overwrite" function that overwrites files created during the printing, network scan, scan-to-email, and LanFax processes. This overwrite process is implemented in accordance with DoD 5200.28-M and will be activated at the completion of each print, network scan, scan to e-mail, or LanFax job, once the MFD is turned back on after a power failure or *on demand* of the MFD system administrator.

The TOE has an "Image Overwrite" function that overwrites files created during the embedded fax process. This overwrite process is implemented as a single-pass zeroization of the embedded fax card flash memory and will be activated at the completion of each embedded fax job, once the MFD is turned back on after a power failure or *on demand* of the MFD system administrator. The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M. LanFax jobs are overwritten on the hard disk after the image is transferred from the Network Controller to Copy Controller, and zeroized on the fax card flash memory once the image has been sent. The Fax mailbox and dial directory are only zeroized when the administrator commands a full On-Demand Image Overwrite (ODIO) operation.

User image files associated with the Copy/Print, Store and Reprint feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job using the 5200.28-M algorithm. The stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite. A standard ODIO overwrites all files written to temporary storage areas of the HDD and zeroizes the temporary storage areas of the fax card flash memory. A full ODIO overwrites those files as well as the Fax mailbox/dial directory, Scan to mailbox

data, and all files that have been stored at the request of a user via Copy/Print, Store and Reprint jobs.

Copy jobs are not written to the hard drive and need not to be overwritten. Copy/Print, Store and Reprint jobs are written to the hard drive so that they may be reprinted at a later time; therefore, they will be overwritten when a full on-demand image overwrite is performed. Embedded FAX jobs are written to flash memory and are overwritten at the completion of each job or on demand of the MFD system administrator. The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M.

#### 1.3.2.2. Authentication (TSF_AUT)

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

#### 1.3.2.3. Network Identification (TSF_NET_ID)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and Embedded Fax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server (a trusted remote IT entity). The user is not required to login to the network; the account is authenticated by the server as a valid user. The remote authentication services supported by the TOE are: LDAP v4, Kerberos (Solaris), Kerberos (Windows 2000/2003), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000/2003).

#### 1.3.2.4. Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit records; the downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

#### 1.3.2.5. Cryptographic Operations (TSF_FCS)

The TOE utilizes data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as

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

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

#### 1.3.2.6. User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing (SSLSec SFP). SSL must be enabled before setting up either IPSec, SNMPv3, or before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. If the system administrator-managed function is enabled, then the TOE creates and enforces the informal security policy model, "All communications to the Web server will utilize SSL (HTTPS)." As provided for in the SSLv3 standard, the TOE will negotiate with the client 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 does not protect scan-to-email, LanFAX or FAX data.

#### 1.3.2.7. User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is generated by the system administrator specifying a series of rules to "accept," "deny," or "drop" packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet. IP Filtering is not available for IPv6, AppleTalk or IPX.

**Note: The TOE cannot enforce the IP Filtering (TSF_FDP_FILTER) security function when it is configured for IPv6, AppleTalk or IPX networks.**

#### 1.3.2.8. User Data Protection – IPSec (TSF_FDP_IPSec)

The TOE implements the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE. Printing clients initiate the establishment of a security association with the MFD. The MFD establishes a security association with the printing client using IPSec "tunnel mode." Thereafter, all IP-based traffic to and from this destination will pass through the IPSec tunnel until either end powers down, or resets, after which the

tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client. IPSec does not protect scan-to-email or FAX data. The transmission of LanFax data over the Ethernet connection is protected by IPSec, but the transmission over the PSTN is not. IPSec is not available for IPv6, AppleTalk or IPX.

**Note: The TOE cannot enforce the IPSec (TSF_FDP_IPSec) security function when it is configured for IPv6, AppleTalk or IPX networks.**

#### 1.3.2.9. Network Management Security (TSF_NET_MGMT)

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

#### 1.3.2.10. Information Flow Security (TSF_FLOW)

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

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

#### 1.3.2.11. Security Management (TSF_FMT)

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

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

Additionally, only authenticated system administrators can assign authorization privileges to users, establish a recurrence schedule for “On Demand” image overwrite, enable/disable SSL support, enable/disable and configure IPSec tunneling, enable/disable and configure SNMPv3, create/install X.509 certificates, enable/disable and download the audit log, enable/disable and configure (rules) IP filtering, or enable/disable and configure IPv6.

#### 1.3.2.12. User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, to support encryption and decryption of designated portions of the hard disk where user files may be stored. Those packages include

provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-128-FIPS-197.

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

### 1.3.3. Evaluated Configuration

In its evaluated configuration, the Image Overwrite Security Package is installed and IIO, ODIO and SSL are enabled on the TOE. The FAX option, if purchased by the consumer, is installed and enabled. All other configuration parameter values are optional. The LanFax option is included in the evaluated configuration of the TOE. Please see http://www.xerox.com/security for more specific information about maintaining the security of this TOE.

# 2. CONFORMANCE CLAIMS

This section describes the conformance claims of this Security Target.

## 2.1. Common Criteria Conformance Claims

The Security Target is based upon

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

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

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

## 2.2. Protection Profile Claims

This Security Target does not claim conformance to any Protection Profile.

## 2.3. Package Claims

This Security Target claims conformance to the EAL2 package augmented with ALC_FLR.3.

# 3. SECURITY PROBLEM DEFINITION

The Security Problem Definition describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

## 3.1. Definitions

### 3.1.1. CC Terms

| | |
|---|---|
| ***Authentication data*** | Information used to verify the claimed identity of a user. |
| ***Authorized User*** | A user who may, in accordance with the SFRs, perform an operation. |
| ***External entity*** | Any entity (human or IT) outside the TOE that interacts (or may interact) 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 in the TOE, 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 in the TOE that performs operations on objects. |
| ***User*** | See external entity. |

### 3.1.2. Subjects

| | |
|---|---|
| ***Human user*** | Any person who interacts with the TOE. |
| ***System Administrator*** | An authorized user who manages the TOE. |

### 3.1.3. Objects

| | |
|---|---|
| ***FAX*** | A generic reference to one of the Fax types supported by the Device (i.e., embedded analog fax (fax board), LanFAX (see below), and Server Fax (not part of the evaluation). |
| ***LanFAX*** | A TOE function in which the data is sent to the device as a print job, but rather than being output as a hardcopy, it is sent out through the embedded analog fax board (optional). |

| | |
|---|---|
| ***Management Interfaces*** | The management interfaces provide access to the related security relevant functions that only system administrators are allowed to use. The management interfaces are accessible via the Local UI and the Web UI. |

### 3.1.4. Information

| | |
|---|---|
| ***Image Data*** | Information on a mass storage device created by the print, scan, or LanFAX processes. |
| ***Latent Image Data*** | Residual information remaining on a mass storage device when a print, scan, or LanFAX job is completed, cancelled, or interrupted. |
| ***User Data*** | Primarily image data, but may also include user commands. |

## 3.2. Assumptions

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

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

**Table 4: Environmental Assumptions**

| Assumption | Description |
|---|---|
| A.INSTALL | The TOE has been delivered and installed by Xerox-authorized representatives using Xerox delivery and installation guidance. The TOE has been configured by the system administrator in accordance with the administrator and user guidance delivered with the TOE as well as the security guidance found at http://www.xerox.com/security. As a part of this installation process, the system administrator has changed the PIN from its default value. The PIN chosen by the administrator consists of at least 8 digits and will be changed at least every 40 days. The Image Overwrite Security accessory is installed and enabled. IIO and ODIO are enabled. Clients will use IPv4 traffic to communicate with the TOE. |
| 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. |

| Assumption | Description |
|---|---|
| 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.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. This also includes the support of a fully functioning I&A mechanism by the environment. |
| 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., SSLv3, IPSec, SNMPv3) and work as advertised. |

# 3.3. Threats

## 3.3.1. Threats Addressed by the TOE

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

**Table 5: Threats Addressed by the TOE**

| Threat | Description |
|---|---|

| | |
|---|---|
| T.RECOVER | A malicious user may attempt to recover temporary or stored document image data using commercially available tools to read its contents.<br>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 document image data can be read/recovered from the fax card flash memory or over the network (e.g. as the result of a purposeful or inadvertent power failure before the data could be erased.) |
| T.COMM_SEC | An attacker may break into an outgoing communications link from the TOE to a remote trusted IT product in order to intercept and/or modify scan-to-mailbox data or SNMP data |
| 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.<br>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.[2]<br>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. Moreover a user may try to use the installed network options (network scanning, scan-to-email, and Embedded Fax) although he is not authorized to do so. |

# 3.4. Organizational Security Policies

This section enumerates the organizational security policies the TOE must comply with:

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

**Table 6: Organizational Security Policy(s)**

| Policy | Description |
|---|---|
| P.COMMS_SEC | The system administrator shall employ TOE supported network security mechanisms (i.e., HTTPS, IPSec ESP and/or AH, SNMPv3, IP filtering) per, and in accordance with, established local site security policy. The environment that directly communicates with the TOE has to be configured in accordance with the TOE policy.<br><br>**Application note:** It is supposed that the customer wants to operate the TOE in its certified configuration. This includes the TOE configured in the way described above. The customer can choose another configuration, but has to be aware that in this case the TOE is not longer in the evaluated configuration. |
| P.HIPAA_OPT | (Appropriate to organizations under HIPAA oversight) All audit log entries (scan) shall 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). The TOE provides the audit log information so that an organization can be compliant; the HIPPA statute requires that personnel actually review the available audit log. |
| P.SSL_ENABLED | Secure Socket layer network security mechanisms shall be supported by the TOE and enabled. |
| P.TRUSTED | The TOE shall accept, establish and use a trusted channel for all incoming IPv4 traffic (IPSec, SSL) when the Client initiates one. |

# 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 scan data transmissions through the TOE that (may) have HIPAA-privileged information. |

| Objectives | Description |
|---|---|
| O.RECOVER | Temporary document image data from a print, network scan, scan-to-email job, LanFax, the Fax mailbox and/or dial directory, Scan to mailbox data, or stored document image data from a Copy/Print, Store and Reprint 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.<br>Temporary document image data from a FAX job must be zeroized in the fax card flash memory immediately after that job is completed or once the TOE is turned back on after a power failure. The embedded fax card flash memory zeroization is not compliant with DoD 5200.28-M.<br>Temporary document image data from the jobs stored on the HDD must also be overwritten on demand in accordance with DoD 5200.28-M (Standard or Full ODIO). The temporary storage for Embedded Faxes (compact flash) must be zeroized at the command ("on demand") of the system administrator when a standard or full ODIO is run. The Fax mailbox and dial directory are only zeroized when the system administrator runs a full ODIO. The embedded fax card flash memory zeroization is not compliant with DoD 5200.28-M. Copy and Embedded 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.<br>The TOE must require that system administrator(s) authenticate with a PIN before allowing access to management functions. The PIN must be obscured as it is entered by the system administrator. The Local UI will be locked for 3 minutes once 3 invalid login attempts have been detected. The WebUI will send an error code after every invalid authentication attempt.<br>The TOE must require authorized users to be identified and authenticated before providing access to installed network options of the TOE. |
| O.CONTROL_ACCESS | The TOE will provide the system administrator with the ability to determine network access/information flow to the TOE for trusted remote IT products. |

| Objectives | Description |
|---|---|
| O.PROTECT_COM | The TOE must protect scan-to-mailbox data and SNMP data from disclosure, or modification, by establishing a trusted channel between the TOE and another trusted IT product over which the data is transported.<br>The TOE must also support, accept, establish and use a trusted channel for all incoming IPv4 traffic (IPSec, SSL) when the Client initiates one. |
| O.PROTECT_DAT | The TOE must protect from disclosure or modification: user data stored for the purpose of reprinting in the future, temporary spool files created from print, fax and scan jobs, and swap files. |

## 4.2. Security Objectives for the Operational 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. |
| OE.NETWORK_I&A | The TOE environment shall provide, per site specific policy, the correct and accurately functioning Identification and Authentication mechanism(s) that are compatible with, and for external use by, the TOE. These mechanisms will be under the same management and physical control as the TOE and are covered by the same management and security policy as the TOE. |
| OE.PROTECT_COM | The TOE environment and remote trusted IT products (which support the external half of all RFC-compliant communication protocols like SSLv3, IPSec and SNMPv3) must protect all IPv4 traffic initiated by the Client from disclosure, or modification, by initiating and establishing a trusted channel between itself and the TOE when SSL is enabled over which the data is transported prior to data transmission. |

| 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.<br>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.<br>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.<br>Non-IPv4 traffic shall not be used by the Clients (IPv6, AppleTalk, IPX). |
| 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, enable SSL, and review audit logs. 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 |

## 4.3. Rationale for Security Objectives

The following table maps the assumptions, threats and OSPs to the objectives for the TOE and the objectives for the operational environment. The mapping will be justified in the subsequent sections of this chapter.

| | O.AUDITS | O.RECOVER | O.FAXLINE | O.MANAGE | O.CONTROL_ACCESS | O.PROTECT_COM | O.PROTECT_DAT | OE.NETWORK | OE.NETWORK_I&A | OE.PROTECT_COM | OE.INSTALL | OE.ACCESS | OE.ADMIN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A.INSTALL** | | | | | | | | | | | X | | |
| **A.ACCESS** | | | | | | | | | | | | X | |
| **A.MANAGE** | | | | | | | | | | | | | X |
| **A.NO_EVIL_ADM** | | | | | | | | | | | X | | X |
| **A.NETWORK** | | | | | | | | X | | | | | |
| **A.SAME_CONTROL** | | | | | | | | | X | | | | |
| **A.EXT_RFC_COMPLIANT** | | | | | | | | | | X | | | |
| **T.RECOVER** | | X | | | X | | X | | | | | | |
| **T.COMM_SEC** | | | | | | X | | | | | | | |
| **T.INFAX** | | | X | | | | | | | | | | |
| **T.OUTFAX** | | | X | | | | | | | | | | |
| **T.USER** | | | | X | | | | X | | | | | |
| **P.COMMS_SEC** | | | | | | X | | | | X | | | X |
| **P.HIPAA_OPT** | X | | | | | | | | | | | | X |
| **P.SSL_ENABLED** | | | | | | X | | | | | | | X |
| **P.TRUSTED** | | | | | | X | | | | X | | | |

### 4.3.1. Coverage of the Assumptions

A.INSTALL — **OE.INSTALL** verbalized the assumption as objective and therefore covers the assumption completely and correctly.

A.ACCESS — **OE.ACCESS** verbalized the assumption as objective and therefore covers the assumption completely and correctly.

A.MANAGE — **OE.ADMIN** verbalized the assumption as objective and therefore covers the assumption completely and correctly.

A.NO_EVIL_ADM — **OE.ADMIN** covers parts of A.NO_EVIL_ADM because “responsible and trustworthy individuals” are “not careless, willfully negligent or hostile.” Furthermore, the individuals must follow the instructions provided in the guidance documents.

**OE.INSTALL** covers the remaining part of

| | |
|---|---|
| | A.NO_EVIL_ADM because the objective ensures that the system administrator configures the TOE according to and will not remove the TOE from the evaluated configuration (especially that the Image Overwrite Security accessory is installed and enabled). |
| A.NEWORK | **OE.NETWORK** verbalized the assumption as objective and therefore covers the assumption completely and correctly. |
| A.SAME_CONTROL | **OE.NETWORK_I&A** covers A.SAME_CONTROL by ensuring the presence within the environment of a fully-functioning I&A mechanism |
| A.EXT_RFC_COMPLIANT | **OE.PROTECT_COM** covers A.EXT_RFC_COMPLIANT by ensuring that a trusted communications channel between the TOE and remote trusted IT products can be established because the remote trusted IT products support the external half of the RFC-compliant communication protocols |

### 4.3.2. Coverage of the Threats

T.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 or in fax card flash memory.

**O.RECOVER** requires that the residual data will be overwritten on the HDD as described in DoD 5200.28-M or zeroized in the fax card flash memory immediately after the job is finished or once the TOE is turned back on after a power failure. Copy and Embedded 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 from the HDD and the Fax card flash memory..

**O.CONTROL_ACCESS** helps counter the threat T.RECOVER because restricted access to TOE network resources helps to prevent recovery attacks from untrusted remote IT products.

| | |
|---|---|
| | **O.PROTECT_DAT** helps counter the threat T.RECOVER because it ensures that user data stored on the hard disk is not recoverable when the disk is removed from the system. |
| T.COMM_SEC | **O.PROTECT_COM** 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 scan-to-mailbox data and SNMP data from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product. |
| T.INFAX | **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. |
| T.OUTFAX | **O.FAXLINE** counters the threat T.OUTFAX because the users of the internal network are not allowed to directly 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** 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. Additionally O.MANAGE counters T.USER by requiring authorized users to be identified and authenticated before providing access to use installed network options of the TOE. 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. |

### 4.3.3. Implementation of Organizational Security Policies

| | |
|---|---|
| P.COMMS_SEC | **O.PROTECT_COM** helps meet P.COMMS_SEC by ensuring that the TOE is configured to establish a fully-compliant trusted channel between the TOE and another remote trusted IT product to protect scan-to-mailbox data |

| | |
|---|---|
| | and SNMP data from disclosure or modification by an attacker. Furthermore, the TOE will accept and establish trusted channels when initiated by the clients.<br><br>OE.PROTECT_COM helps meet P.COMMS_SEC by ensuring that the TOE environment and trusted IT products are configured according to the TOE policy to protect client-initiated IPv4 traffic to the TOE.<br><br>**OE.ADMIN** helps meet P.COMMS_SEC by ensuring that local site security policies have been complied with by a competent administrator. |
| P.HIPAA_OPT | **O.AUDITS** helps satisfy P.HIPAA_OPT by ensuring that log entries are provided by the TOE for periodic review by a competent administrator (**OE.ADMIN**), 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.SSL_ENABLED | **O.PROTECT_COM** helps meet P.SSL_ENABLED by ensuring that the TOE supports SSL. **OE.ADMIN** supports P.SSL_ENABLED by ensuring that SSL is enabled. |
| P.TRUSTED | **O.PROTECT_COM** helps meet P.TRUSTED by ensuring that the TOE supports the mechanisms to protect incoming IPv4 communication.<br>**OE.PROTECT_COM** helps meet P.TRUSTED by ensuring that a fully RFC compliant trusted channel between the TOE and another remote trusted IT product will be initiated by the client to protect all incoming IPv4 traffic to the TOE from disclosure or modification by an attacker attempting to intercept communications between the TOE and the remote trusted IT product. |

# 5. SECURITY REQUIREMENTS

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

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

## 5.1. Conventions

All operations performed on the Security Functional Requirements or the Security Assurance Requirements need to be identified. For this purpose the following conventions shall be used.

- Assignments will be written in normal text with brackets: [normal]
- Selections will be written in underlined and italic text
- Refinements will be written bold
- Iterations will be performed on components and functional elements. The component ID defined by the Common Criteria (e.g. FDP_IFC.1) will be extended by an ID for the iteration (e.g. “(SSL)”). The resulting component ID would be “FDP_IFC.1 (SSL)”.
- Where an iteration is identified in rationale discussion as “all”, the statement applies to all iterations of the requirement (e.g. “FCS_CKM.1 (all)”)

## 5.2. Security Policies

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

**Note: The TOE cannot enforce the IP Filtering (TSP_FILTER), and IPSec (TSP_IPSEC) security policies when it is configured for IPv6, AppleTalk or IPX networks.**

### 5.2.1. User Data Protection Policy (TSP_IOW)

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

- Temporary document image data from a print, network scan, LanFax or scan-to-email job must be overwritten on the hard disk drive in accordance with DoD 5200.28-M immediately after that job is completed. Temporary document image data from a FAX job must be overwritten (zeroized) in fax card flash memory immediately after that job is completed. The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M.
- All temporary document image data of abnormally terminated jobs on the HDD 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.
- The space on the hard disk drive reserved for the Scan to mailbox data, and Copy/Print, Store and Reprint image data must be overwritten in accordance with DoD 5200.28-M, if the system administrator has invoked the On Demand Image Overwrite function.
- The space on the fax card flash memory must be zeroized, if the system administrator has invoked the On Demand Image Overwrite function and when the TOE is powered on after a power failure.
- Document image data of copy and Embedded FAX jobs must not be written to the hard disk drive.

### 5.2.2. Information Flow Control Policy (TSP_FLOW)

The security function “Information Flow” (TSF_FLOW) (see section 01.3.2.10) 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 copy controller (SIP) (see section 1.3.2.10) may copy image information and job data (e.g. the telephone number of the other fax machine) from and to a shared memory area on the FAX board.
- RECEIVING FAX: The FAX board must have terminated the PSTN connection before informing the copy controller about the fax currently received.
- SENDING FAX: The copy controller must have finished the copy operation of the fax image to the shared memory area of the FAX board before informing the FAX board to send the fax.

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

### 5.2.3. SSLSec SFP (TSP_SSL)

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

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

### 5.2.4. IP Filter SFP (TSP_FILTER)

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

- SUBJECTS: External entities that send network traffic to the TOE.
- INFORMATION: All IPv4-based traffic to and from that destination.
- OPERATIONS: Pass network traffic.

### 5.2.5. IPSec SFP (TSP_IPSEC)

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

- SUBJECTS: Printing clients.
- INFORMATION: All lpr and port 9100 traffic from that destination.
- OPERATIONS: Print jobs.

### 5.2.6. SNMPSec SFP (TSP_SNMP)

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

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

### 5.2.7. PrivUserAccess SFP (TSP_FMT)

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

## 5.3. Security Functional Requirements

The TOE satisfies the SFRs delineated in Table 9. The rest of this section contains a description of each component and any related dependencies.

**Table 9: TOE Security Functional Requirements**

| Functional Component ID | Functional Component Name |
|---|---|
| FAU_GEN.1 | Audit data generation |
| FAU_SAR.1 | Audit review |
| FAU_SAR.2 | Restricted audit review |
| FAU_STG.1 | Protected audit trail storage |
| FAU_STG.4 | Prevention of audit data loss |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.2 | Cryptographic key distribution |
| FCS_COP.1 | Cryptographic operation |
| FCS_CKM.4 | Cryptographic key destruction |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Access control functions |
| FDP_IFC.1 | Subset information flow control |
| FDP_IFF.1 | Simple security attributes |
| FDP_RIP.1 | Subset residual information protection |
| FDP_UCT.1 | Basic data exchange confidentiality |
| FDP_UIT.1 | Data exchange integrity |
| FIA_AFL.1 | Authentication failure handling |
| FIA_UAU.2 | User authentication before any action |
| FIA_UAU.7 | Protected authentication feedback |
| FIA_UID.2 | User identification before any action |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialisation |

| Functional Component ID | Functional Component Name |
|---|---|
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of management functions |
| FMT_SMR.1 | Security Roles |
| FPT_STM.1 | Reliable time stamp |
| FTP_ITC.1 | Inter-TSF trusted channel |
| FTP_TRP.1 | Trusted Path |

## 5.3.1. Class FAU: Security Audit

### 5.3.1.1. FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamp

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 (if applicable), 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 entries specified at the top of Table 10 below].

**Table 10: Audit Events**

| |
|---|
| The audit log will have the following fixed size entries:<br>• Entry number (an integer value from 1 to the number of entries in the audit log)<br>• Event Date (mm/dd/yy)<br>• Event Time (hh:mm:ss)<br>• 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 Standard started | Device name; Device serial number |
| 4 | ODIO Standard 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 |
| 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 |
| 14 | LanFax job | Job name; User Name; Completion Status; IIO status; Accounting User ID; Accounting Account ID; total-fax-recipient-phone-numbers; fax-recipient-phone-numbers. |
| 16 | ODIO Full started | Device name<br>Device serial number |
| 17 | ODIO Full complete | Device name<br>Device serial number |

| | | |
|---|---|---|
| | | Overwrite Status |
| 20 | Scan to Mailbox job | Job name or Dir name<br>User Name<br>Completion Status<br>IIO status |
| 21 | Delete File/Dir | Job name or Dir name<br>User Name<br>Completion Status<br>IIO status |
| 23 | Scan to Home | UserName<br>Device name<br>Device serial number<br>Completion Status (Enabled/Disabled) |
| 30 | SA login | Device name<br>Device serial number<br>Completion Status (Success or Failed) |
| 31 | User Login | UserName<br>Device name<br>Device serial number<br>Completion Status (Success or Failed) |
| 32 | Service Login | Service name<br>Device name<br>Device serial number<br>Completion status (Success or Failed). |
| 33 | Audit log download | UserName<br>Device name<br>Device Serial Number<br>Completion status (Success or Failed). |
| 34 | IIO feature status | UserName<br>Device name<br>Device serial number<br>IIO Status (enabled or disabled) |
| 35 | SA pin changed | UserName<br>Device name<br>Device serial number<br>Completion status |
| 36 | Audit log Transfer | UserName<br>Device name<br>Device serial number<br>Completion status |
| 37 | SSL | UserName<br>Device name<br>Device serial number<br>Completion status (Enabled/Disabled). |

| | | |
|---|---|---|
| 38 | X509 certificate | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Created/uploaded/Downloaded). |
| 39 | IP sec | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Configured/enabled/disabled). |
| 40 | SNMPv3 | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Configured/enabled/disabled). |
| 41 | IP Filtering Rules | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Configured/enabled/disabled). |
| 42 | Network Authentication | UserName<br>Device name<br>Device serial number<br>Completion Status (Enabled/Disabled) |
| 43 | Device clock | UserName<br>Device name<br>Device serial number<br>Completion Status (time changed/date changed) |
| 44 | SW upgrade | Device name<br>Device serial number<br>Completion Status (Success, Failed) |
| 45 | Cloning | Device name<br>Device serial number<br>Completion Status (Success, Failed) |
| 46 | Secure scanning | Device name<br>Device serial number<br>Completion Status (Certificate validation<br>success, failed) |
| 50 | Process crash | Device name<br>Device serial number<br>Process name |
| 51 | ODIO scheduled | Device name<br>Device serial number |

| | | |
|---|---|---|
| | | ODIO type (Standard)<br>Scheduled time<br>ODIO status<br>(Started/Completed/canceled)<br>Completion Status<br>(Success/Failed/Canceled) |

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

#### 5.3.1.2. FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

#### 5.3.1.3. FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

#### 5.3.1.4. FAU_STG.1 Protected audit trail storage

Hierarchical to: None.

Dependencies: FAU_GEN.1 Audit data generation

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

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

#### 5.3.1.5. FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3.

Dependencies: FAU_STG.1 Protected audit trail storage

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

## 5.3.2. Class FCS: Cryptographic Support (SSL Specific)

### 5.3.2.1. FCS_CKM.1 (SSL 1) Cryptographic key generation

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [as defined in the SSL v3 standard] and specified cryptographic key sizes [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 (SSL2)].

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

### 5.3.2.2. FCS_CKM.1 (SSL 2) Cryptographic key generation

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [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].

**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.

#### 5.3.2.3. FCS_CKM.2 (SSL 1) Cryptographic key distribution

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.2.1 | The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA encrypted exchange of session keys for SSL handshake] that meet the following: [SSLv3 standard]. |

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

#### 5.3.2.4. FCS_CKM.2 (SSL 2) Cryptographic key distribution

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.2.1 | The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [digital certificates for public RSA keys] that meet the following: [certificate format given in X.509v3]. |

#### 5.3.2.5. FCS_COP.1 (SSL 1) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [digital signature generation and verification] in accordance with a specified cryptographic |

| | |
|---|---|
| | algorithm [RSA] 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<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |

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

#### 5.3.2.6. FCS_COP.1 (SSL 2) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [RC4] and cryptographic key sizes [128 bit] that meet the following: [SSLv3 standard – SSL_RSA_WITH_RC4_128_SHA cipher suite]. |

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

### 5.3.3. Class FCS: Cryptographic Support (IPSec Specific)

#### 5.3.3.1. FCS_CKM.1 (IPSEC) Cryptographic key generation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1 | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple Data Encryption Standard (3DES-EDE)] and specified cryptographic key sizes [3 unique 56-bit keys] that meet the following: [FIPS-42-2, FIPS-74, FIPS-81]. |

### 5.3.3.2. FCS_COP.1 (IPSEC 1) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [<br><br>a) IPSec Security Association data encryption/decryption specified by IKE in RFC2409 as defined in TSP_IPSEC; and<br><br>b) IPSec ESP bulk data encryption/decryption specified by IKE in RFC2406 as defined in the TSP_IPSEC]<br><br>in accordance with a specified cryptographic algorithm [3DES-EDE] and cryptographic key sizes [168 bits] that meet the following: [ FIPS-42-2, FIPS-74, FIPS-81]. |

### 5.3.3.3. FCS_COP.1 (IPSEC 2) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [N/A] that meet the following: [RFC1321]. |

### 5.3.3.4. FCS_COP.1 (IPSEC 3) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [cryptographic checksum generation and secure hash (message digest) computation] in accordance with a |

specified cryptographic algorithm [SHA-1] and cryptographic key sizes [N/A] that meet the following: [FIPS-186].

### 5.3.4. Class FCS: Cryptographic Support (SNMPv3 Specific)

#### 5.3.4.1. FCS_CKM.1 (SNMP) Cryptographic key generation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1 | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [DES] and specified cryptographic key sizes [64 bit] that meet the following: [generation of keys as defined in the SNMPv3 standard with the cipher suites defined in FCS_COP.1 (SNMP)]. |

#### 5.3.4.2. FCS_COP.1 (SNMP) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [hashing and verification] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [none] that meet the following: [SNMPv3 standard]. |

### 5.3.5. Class FCS: Cryptographic Support (Disk Encryption Specific)

#### 5.3.5.1. FCS_CKM.1 (UDE) Cryptographic key generation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1 | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and |

specified cryptographic key sizes [128 bit] that meet the following: [randomization of network interface MAC address upon boot up].

#### 5.3.5.2. FCS_COP.1 (UDE) Cryptographic operation

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1 | The TSF shall perform [encryptions and decryption] **on user data stored on the HDD** in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bit] that meet the following: [none]. |

### 5.3.6. Class FCS: Cryptographic Support (General)

#### 5.3.6.1. FCS_CKM.4 Cryptographic key destruction

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] |
| FCS_CKM.4.1 | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [semiconductor memory state loss at power-down, semiconductor memory zeroization at power-up] that meets the following: [None]. |

### 5.3.7. Class FDP: User Data Protection

#### 5.3.7.1. FDP_ACC.1 Subset access control

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |
| FDP_ACC.1.1 | The TSF shall enforce the [PrivUserAccess SFP] on [<br>• Subjects: authorized users;<br>• Object: functions accessible via WebUI and Local UI;<br>• Operations: access management interfaces]. |

### 5.3.7.2. FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

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

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

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

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

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

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

### 5.3.7.3. FDP_IFC.1 (IOW) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

subjects: the hard disk drive, fax card flash memory
information: image information
operations: storage and erase of the image information].

### 5.3.7.4. FDP_IFF.1 (IOW) Simple security attributes

Hierarchical to: No other components.

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

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

- MFD Job
  - Type of the job (print; network scan; scan-to-email; copy; FAX; Copy/Print, Store and Reprint)
- image information of the job
  - no security attributes].

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

- A MFD job of the type print, network scan, LanFax or scan-to-email may store image information in the reserved space on the hard disk drive.
- A MFD job of the type fax may store image information in the Fax compact flash memory.
- A MFD job of the type Copy/Print, Store and Reprint may store image information in a reserved space of the hard disk drive for the purpose of being reprinted at a later time].

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

- When the TOE is turned back on after a power failure, all temporary document image data stored on the hard disk or fax card flash memory of abnormally terminated jobs shall be overwritten according to DoD 5200.28-M (HDD) or respectively zeroized (flash memory).
- Once the system administrator has invoked standard ODIO, the space on the hard disk drive reserved for temporary and stored 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. The temporary document image data on the fax card flash memory shall be zeroized until the complete space is erased or the function is canceled by the system administrator.
- Once the system administrator has invoked a full ODIO, the space on the hard disk drive reserved for temporary and stored document image and directory 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. The temporary document image data, the Fax

mailbox and the dial directory on the fax card flash memory shall be zeroized until the complete space is erased or the function is canceled by the system administrator.

].

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

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

- Except for Copy/Print, Store and Reprint jobs, a MFD job of the type copy or embedded fax must not store image information on the hard disk drive.].

### 5.3.7.5. FDP_IFC.1 (FLOW) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [information flow control policy TSP_FLOW] on [
subjects: SIP, the network controller, the FAX board
information: fax image information and job data, command messages
operations: receiving a fax, sending command messages, receiving command messages, copy operation of FAX image data, sending a FAX
].

### 5.3.7.6. FDP_IFF.1 (FLOW) Simple security attributes

Hierarchical to: No other components.

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

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

- the copy controller (SIP)
  - copy operation from/to the shared memory area of the FAX board in progress or not
- the network controller
  - no security attributes
- the FAX board

  - PSTN port in use or not
- fax image information and job data
  - address of the memory where the data is stored (on the copy controller or on the FAX board)
- command messages
  - Type of the command message between FAX board and copy controller

]

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

- The copy controller is allowed to copy fax image information and job data from the shared memory of the FAX board to its own memory.
- The copy controller is allowed to copy fax image information and job data from its own memory to the shared memory of the FAX board.
- The FAX board is allowed to send out a fax over PSTN once the copy controller has signaled the end of the copy operation to the shared memory area.
- The FAX board is allowed to signal the copy controller “Fax received” once the PSTN connection has been terminated.
- The network controller is allowed to send image information and respective commands to the copy controller.

].

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

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

].

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

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

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

].

### 5.3.7.7. FDP_IFC.1 (FILTER) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

- Subjects: External entities that send traffic to the TOE;
- Information: All IPv4-based traffic to/from that source/destination;
- Operations: send or receive network traffic].

### 5.3.7.8. FDP_IFF.1 (FILTER) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization.

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

- Subjects: External entities that send traffic to the TOE
  - IPv4 address,
- Information: IPv4 Package
  - Source IP address, protocol used (TCP or UDP), destination TCP or UDP port].

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

- The source IPv4 address matches a rule in the TOE's rule base
- If configured, the destination transport layer port matches a rule in the TOE's rule base.]

FDP_IFF.1.3 The TSF shall enforce the [implicit allow if no rules have been defined].

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

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

*Application Note: When custom rules have not been defined by the system administrator, the default rule (allow all traffic) will apply. Because it is a wildcard rule, all IPv4 addresses, ports and protocols (either TCP or UDP) will be a match for allowed traffic.*

### 5.3.7.9. FDP_IFC.1 (IPSEC) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

- Subjects: Printing clients;
- Information: All IPv4-based traffic from that destination/source;
- Operations: Printing].

### 5.3.7.10. FDP_IFF.1 (IPSEC) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

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

- Subjects: Printing clients
  - IPv4 address;
- Information: Print jobs
  - Issuer (printing client) of this print job].

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

- Printing clients initiate the establishment of a security association with the MFD
- The MFD establishes a security association with the printing client using IPSec “tunnel mode”
- The print jobs to the TOE passes the IPSec tunnel].

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

| | |
|---|---|
| FDP_IFF.1.4 | The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules based on security attributes that explicitly authorize information flows]. |
| FDP_IFF.1.5 | The TSF shall explicitly deny any information flow based on the following rules: [none]. |

### 5.3.7.11. FDP_IFC.1 (SSL) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

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

### 5.3.7.12. FDP_IFF.1 (SSL) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

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

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

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

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

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

| | |
|---|---|
| FDP_IFF.1.4 | The TSF shall explicitly authorize an information flow based o the following rules: [no additional rules based on security attributes that explicitly authorize information flows]. |
| FDP_IFF.1.5 | The TSF shall explicitly deny any information flow based on the following rules: [HTTP traffic without an SSL tunnel]. |

### 5.3.7.13. FDP_IFC.1 (SNMP) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

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

### 5.3.7.14. FDP_IFF.1 (SNMP) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

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

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

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

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

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

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

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

### 5.3.7.15. FDP_RIP.1 (IOW 1) Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of **temporary image files will be overwritten according to DoD 5200.28-M** upon the *deallocation of the **temporary image files** from* the following objects: [print, network scan or scan-to-email job].

*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-email job is finished.*

### 5.3.7.16. FDP_RIP.1 (IOW 2) Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of **temporary image files will be overwritten with zeroes** upon the *deallocation of the **temporary image files** from* the following objects: [embedded fax job].

*Application Note: The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M.*

### 5.3.7.17. FDP_RIP.1 (IOW 3) Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

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

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

### 5.3.7.18. FDP_UCT.1 (IPSEC) Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]

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

### 5.3.7.19. FDP_UIT.1 (IPSEC) Data exchange integrity

Hierarchical to: No other components

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

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

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

### 5.3.7.20. FDP_UCT.1 (SSL) Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]

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

### 5.3.7.21. FDP_UIT.1 (SSL) Data exchange integrity

Hierarchical to: No other components

| | |
|---|---|
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path] |
| FDP_UIT.1.1 | The TSF shall enforce the [SSLSec SFP] to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and/or replay* errors. |
| FDP_UIT.1.2 | The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and/or replay* has occurred. |

#### 5.3.7.22. FDP_UCT.1 (SNMP) Basic data exchange confidentiality

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | [FDP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control or<br>FDP_IFC.1 Subset information flow control] |
| FDP_UCT.1.1 | The TSF shall enforce the [SNMPSec SFP] to be able to *transmit and receive* user data in a manner protected from unauthorized disclosure. |

#### 5.3.7.23. FDP_UIT.1 (SNMP) Data exchange integrity

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

### 5.3.8. Class FIA: Identification and Authentication

#### 5.3.8.1. FIA_AFL.1 (AUT 1) Authentication failure handling

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FIA_UAU.1 Timing of authentication |

| | |
|---|---|
| FIA_AFL.1.1 | The TSF shall detect when [3] unsuccessful authentication attempts occur related to [authentication at the local user interface]. |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [lockout the SA login for a period of at least 3 minutes on the Local User Interface]. |

#### 5.3.8.2. FIA_AFL.1 (AUT 2) Authentication failure handling

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FIA_UAU.1 Timing of authentication |
| FIA_AFL.1.1 | The TSF shall detect when [3] unsuccessful authentication attempts occurs related to [authentication at the Web User Interface]. |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [lockout the SA login for a period of 5 minutes on the Web User Interface]. |

#### 5.3.8.3. FIA_UAU.2 User authentication before any action

| | |
|---|---|
| Hierarchical to: | FIA_UAU.1 Timing of Authentication |
| Dependencies: | FIA_UID.1 Timing of Identification |
| FIA_UAU.2.1 | The TSF shall require each **system administrator and authorized user** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **system administrator and authorized user**. |

*Application Note: This SFR represents two separate I&A mechanisms: one for the System Administrator, which is completely implemented in the TOE and one for the Authorized User, which only enforces that the I&A-mechanism implemented in the TOE environment will be used before granting access.*

#### 5.3.8.4. FIA_UAU.7 Protected authentication feedback

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FIA_UAU.1 Timing of Authentication |
| FIA_UAU.7.1 | The TSF shall provide only [obscured feedback] to the **system administrator** while the authentication is in progress. |

#### 5.3.8.5. FIA_UID.2 User identification before any action

| | |
|---|---|
| Hierarchical to: | FIA_UID.1 Timing of Identification |
| Dependencies: | No dependencies |
| FIA_UID.2.1 | The TSF shall require each **system administrator and authorized user** to be successfully identified before allowing any other TSF- |

mediated actions on behalf of that system administrator and authorized user.

*Application Note: This SFR represents two separate I&A mechanisms: one for the System Administrator, which is completely implemented in the TOE and one for the Authorized User, which only enforces that the I&A-mechanism implemented in the TOE environment will be used before granting access.*

## 5.3.9. Class FMT: Security Management

### 5.3.9.1. FMT_MOF.1 (FMT 1) Management of security functions behavior

Hierarchical to: No other components

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

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

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

to [the system administrator].

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

Hierarchical to: No other components

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

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

- Change PIN,
- Invoke ODIO,
- Abort ODIO
- Assign authorization privileges to users

- Establish IPv4 address and TCP Port filtering rules
- Create/install X.509 certificates
- Create/install IPSec shared secrets
- Create/install SNMPv3 shared secrets]

to [the system administrator].

#### 5.3.9.3. FMT_MSA.1 (IOW) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] to restrict the ability to *change default, modify, delete [all security attributes]* to [nobody].

#### 5.3.9.4. FMT_MSA.3 (IOW) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [User Data Protection Policy (TSP_IOW)] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.

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

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

#### 5.3.9.5. FMT_MSA.1 (FLOW) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [information flow control policy TSP_FLOW] to restrict the ability to *change default, query, modify, delete [all security attributes]* to [nobody].

### 5.3.9.6. FMT_MSA.3 (FLOW) Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [information flow control policy TSP_FLOW] to provide *[fixed]* default values for security attributes that are used to enforce the SFP.

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

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

### 5.3.9.7. FMT_MTD.1 (AUT) Management of TSF data

Hierarchical to: No other components

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

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

- Audit log]

to [the system administrator].

### 5.3.9.8. FMT_MTD.1 (SNMP) Management of TSF data

Hierarchical to: No other components

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

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

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

to [the system administrator].

### 5.3.9.9. FMT_MTD.1 (FILTER)Management of TSF data

Hierarchical to: No other components

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

FMT_MTD.1.1 The TSF shall restrict the ability to *query*, *modify*, *delete*, [*create*] the [

- IP filter rules]

to [the system administrator].

### 5.3.9.10. FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

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

- Enable/disable Immediate Image Overwrite (IIO) [TSF_IOW] (Local User Interfaces);
- Enable/disable On Demand Image Overwrite (ODIO) [TSF_IOW] (Local User Interface),
- Change PIN (Local User Interface);
- Invoke ODIO [TSF_IOW] (Web and Local User Interfaces);
- Abort ODIO [TSF_IOW] (only Local User Interface, and only if invoked at the Local User Interface)
- Create a recurrence schedule for "On Demand" image overwrite (Web User Interface);
- Enable/disable audit function (Web User Interface);
- Transfer the audit records (if audit is enabled) to a remote trusted IT product (Web User Interface);
- Enable/disable SSL (Web User Interface)`;
- Create/upload/download X.509 certificates (Web User Interface);
- Enable/disable and configure IPSec tunneling (Web User Interface);
- Enable/disable and configure SNMPv3 (Web User Interface);

- Enable/disable and configure (specify the IPv4 address and/or IPv4 address range, port and port range for remote trusted IT products (presumed) allowed to connect to the TOE via the network interface) IP filtering] (Web User Interface);
- Enable/disable and configure IPv6 (Web User Interface).

#### 5.3.9.11. FMT_SMR.1 Security roles

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

### 5.3.10. Class FPT: Protection of the TSF

#### 5.3.10.1. FPT_STM.1 Reliable time stamps

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No Dependencies |
| FPT_STM.1.1 | The TSF shall be able to provide reliable time stamps. |

### 5.3.11. Class FTP: Trusted path/channels

#### 5.3.11.1. FTP_ITC.1 Inter-TSF trusted channel

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FTP_ITC.1.1 | The TSF shall provide a communication channel between itself and another 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]. |

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |

| | |
|---|---|
| FTP_TRP.1.1 | The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*. |
| FTP_TRP.1.2 | The TSF shall permit *remote users* to initiate communication via the trusted path. |
| FTP_TRP.1.3 | The TSF shall require use of the trusted path for [<br>• *Print jobs submitted via lpr or port 9100*]. |

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FTP_TRP.1.1 | The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*. |
| FTP_TRP.1.2 | The TSF shall permit *remote users* to initiate communication via the trusted path. |
| FTP_TRP.1.3 | The TSF shall require use of the trusted path for [<br>• *Print jobs and LanFax jobs submitted via Web UI,*<br>• *the security management functions available to the system administrator from the Web UI*]. |

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FTP_TRP.1.1 | The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification or disclosure*. |
| FTP_TRP.1.2 | The TSF shall permit *remote users and the TSF* to initiate communication via the trusted path. |
| FTP_TRP.1.3 | The TSF shall require use of the trusted path for [ *SNMP messages*]. |

# 5.4. TOE Security Assurance Requirements

Table 11 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2 and includes the augmented SAR, ALC_FLR.3. The SARs are not iterated or refined from Part 3.

**Table 11: EAL2 (augmented with ALC_FLR.3) Assurance Requirements**

| Assurance Component ID | Assurance Component Name | Dependencies |
|---|---|---|
| ADV_ARC.1 | Security architecture description | ADV_FSP.1, ADV_TDS.1 |
| ADV_FSP.2 | Security-enforcing functional specification | ADV_TDS.1 |
| ADV_TDS.1 | Basic design | ADV_FSP.2 |
| AGD_OPE.1 | Operational user guidance | ADV_FSP.1 |
| AGD_PRE.1 | Preparative procedures | None |
| ALC_CMC.2 | Use of a CM system | ALC_CMS.1 |
| ALC_CMS.2 | Parts of the TOE CM coverage | None |
| ALC_DEL.1 | Delivery procedures | None |
| ALC_FLR.3 | Systematic flaw remediation | None |
| ASE_CCL.1 | Conformance claims | ASE_INT.1, ASE_ECD.1, ASE_REQ.1 |
| ASE_ECD.1 | Extended components definition | None |
| ASE_INT.1 | ST introduction | None |
| ASE_OBJ.2 | Security objectives | ASE_SPD.1 |
| ASE_REQ.2 | Derived security requirements | ASE_OBJ.2, ASE_ECD.1 |
| ASE_SPD.1 | Security problem definition | None |
| ASE_TSS.1 | TOE summary specification | ASE_INT.1, ASE_REQ.1, ADV_FSP.1 |
| ATE_COV.1 | Evidence of coverage | ADV_FSP.2, ATE_FUN.1 |
| ATE_FUN.1 | Functional testing | ATE_COV.1 |
| ATE_IND.2 | Independent testing-sample | ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1 |
| AVA_VAN.2 | Vulnerability analysis | ADV_ARC.1, ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1 |

# 5.5. Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

# 5.6. Explicitly Stated Requirements for the TOE

There are no explicitly stated requirements for the TOE.

# 5.7. Rationale for Security Functional Requirements

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

| | O.AUDITS | O.RECOVER | O.FAXLINE | O.MANAGE | O.CONTROL_ACCESS | O.PROTECT_COM | O.PROTECT_DAT |
|---|---|---|---|---|---|---|---|
| **FDP_IFC.1 (FLOW)** | | | X | | | | |
| **FDP_IFF.1 (FLOW)** | | | X | | | | |
| **FDP_IFC.1 (FILTER)** | | | | | X | | |
| **FDP_IFF.1 (FILTER)** | | | | | X | | |
| **FDP_IFC.1 (IPSEC)** | | | | | | X | |
| **FDP_IFF.1 (IPSEC)** | | | | | | X | |
| **FDP_IFC.1 (SSL)** | | | | | | X | |
| **FDP_IFF.1 (SSL)** | | | | | | X | |
| **FDP_IFC.1 (SNMP)** | | | | | | X | |
| **FDP_IFF.1 (SNMP)** | | | | | | X | |
| **FDP_RIP.1 (IOW 1)** | | X | | | | | X |
| **FDP_RIP.1 (IOW 2)** | | X | | | | | X |
| **FDP_RIP.1 (IOW 3)** | | X | | | | | X |
| **FDP_UCT.1 (IPSEC)** | | | | | | X | |
| **FDP_UIT.1 (IPSEC)** | | | | | | X | |
| **FDP_UCT.1 (SSL)** | | | | | | X | |
| **FDP_UIT.1 (SSL)** | | | | | | X | |
| **FDP_UCT.1 (SNMP)** | | | | | | X | |
| **FDP_UIT.1 (SNMP)** | | | | | | X | |
| **FIA_AFL.1 (AUT 1)** | | | | X | | | |
| **FIA_AFL.1 (AUT 2)** | | | | X | | | |
| **FIA_UAU.2** | | | | X | | | |
| **FIA_UAU.7** | | | | X | | | |
| **FIA_UID.2** | | | | X | | | |
| **FMT_MOF.1 (FMT 1)** | | X | | X | X | X | |
| **FMT_MOF.1 (FMT 2)** | | X | | X | X | X | |
| **FMT_MSA.1 (IOW)** | | X | | | | | |
| **FMT_MSA.3 (IOW)** | | X | | | | | |
| **FMT_MSA.1 (FLOW)** | | X | X | | | | |
| **FMT_MSA.3 (FLOW)** | | X | X | | | | |
| **FMT_MTD.1 (AUT)** | | | | X | | | |
| **FMT_MTD.1 (SNMP)** | | | | X | | X | |
| **FMT_MTD.1 (FILTER)** | | | | X | X | | |

| | O.AUDITS | O.RECOVER | O.FAXLINE | O.MANAGE | O.CONTROL_ACCESS | O.PROTECT_COM | O.PROTECT_DAT |
|---|---|---|---|---|---|---|---|
| **FMT_SMF.1** | | **X** | | **X** | **X** | **X** | |
| **FMT_SMR.1** | | **X** | | **X** | **X** | **X** | |
| **FPT_STM.1** | **X** | | | | | **X** | |
| **FTP_ITC.1** | | | | | | **X** | |
| **FTP_TRP.1 (IPSEC)** | | | | | | **X** | |
| **FTP_TRP.1 (SSL)** | | | | | | **X** | |
| **FTP_TRP.1 (SNMP)** | | | | | | **X** | |

| | |
|---|---|
| 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.<br>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.<br>FAU_STG.1 and FAU_STG.4 ensure that the TOE is able to prevent unauthorized modification of audit trail records and, when the audit trail file is full, is able to overwrite the oldest stored audit records without other modification to stored records.<br>FPT_STM.1 ensures that the TOE provides a reliable timestamp for inclusion in the audit log. |
| O.RECOVER | FDP_RIP.1 (IOW 1) , FDP_RIP.1 (IOW 2) ensure that residual temporary document data does not remain on the mass storage device or compact flash memory once the corresponding job has completed processing.<br>FDP_RIP.1 (IOW 3) ensures that residual stored document data does not remain on the mass storage device once the system administrator has determined that the stored jobs and data are no longer necessary.<br>FDP_IFF.1 (IOW) together with FDP_IFC.1 (IOW) ensures that all temporary document image data of abnormally terminated jobs will be overwritten once the TOE is turned back on after a power failure. Additionally, these two requirements ensure that the complete space reserved for temporary document |

| | |
|---|---|
| | image data can be overwritten "on demand" by the system administrator.<br><br>FMT_SMF.1 requires that there is a possibility to invoke this ODIO function. FMT_MOF.1 (FMT 1) specifies that the function can be enabled or disabled by the system administrator. FMT_MOF.1 (FMT 2) restricts the use of this function to the system administrator. FMT_SMR.1 manages the role "system administrator".<br><br>FMT_MSA.1 (FLOW) requires that no one be able to change or delete the security attributes.<br><br>FMT_MSA.3 (IOW), FMT_MSA.3 (FLOW) and FMT_MSA.1 (IOW) define the space where the temporary document image data can be stored and deny the modification of this space by anyone. FDP_IFF.1 (IOW) and FDP_IFC.1 (IOW) also ensure that Copy and Fax jobs will not be written to the HDD at all. |
| O.FAXLINE | FDP_IFC.1 (FLOW) and FDP_IFF.1 (FLOW) define the rules according to which an information flow between network controller, copy controller and FAX board (if installed) is allowed. By implementing a store-and-forward principle in both directions, a direct interconnection between the PSTN and the internal network is not possible.<br><br>FMT_MSA.3 (FLOW) and FMT_MSA.1 (FLOW) define the possible command types and the address spaces of the copy controller and the FAX board. Nobody shall be able to modify these parameters. |
| O.MANAGE | FAU_GEN.1 ensures that the TOE is able to generate time-stamped audit records of a specified set of security-relevant events related to TOE operations.<br><br>FMT_SMF.1 ensures that the security management functions (i.e., enable/disable IIO and ODIO, change system administrator PIN, invoke/abort ODIO, enable/disable Network Authentication, enable/disable Audit Logging, enable/disable SSL, enable/disable IP Filtering, enable/disable IPSec, and enable/disable SNMPv3) are available on the TOE.<br><br>FMT_MOF.1 (FMT 1) and FMT_MOF.1 (FMT 2) restrict the access to these management functions to the system administrator. FMT_SMR.1 manages the role "system administrator".<br><br>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.<br><br>FIA_UAU.2 and FIA_UID.2 ensure that the TOE enforces authorized users to identify and authenticate before being able to use the installed network options of the TOE.<br><br>FIA_AFL.1 (AUT 1) ensures that the TOE takes specific and immediate self-protection action when the set threshold of unsuccessful login attempts by the |

| | |
|---|---|
| | System Administrator is reached for the Local User Interface.<br><br>FIA_AFL.1 (AUT 2) provides an appropriate error message to the user's web browser and locks the interface for a certain time when the set threshold of unsuccessful login attempts by the System Administrator is reached for the Web User Interface.<br><br>FMT_MTD.1 (all) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to query, modify, delete, create, or install specified security attributes, keys and certificates, and IP filter rules. |
| O.CONTROL_ ACCESS | 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.<br><br>FDP_ACC.1 and FDP_ACF.1 ensure that the TOE enforces the PrivUserAccess SFP on subjects, objects, information, and operations and applies specific rules on all operations involving controlled subjects and objects, limiting access to management interfaces to the System Administrator.<br><br>FDP_IFC.1 (FILTER) and FDP_IFF.1 (FILTER) ensure that the IP_Filter SFP is enforced to control and protect information flow between controlled subjects (IPv4 address, destination port, etc.) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner.<br><br>FMT_SMF.1 requires that there is a possibility to invoke the IP Filter function. FMT_MOF.1 (FMT 1) specifies that the function can be enabled or disabled by the system administrator. FMT_MOF.1 (FMT 2) restricts the use of this function to the system administrator. FMT_SMR.1 manages the role "system administrator".<br><br>FMT_MTD.1 (FILTER) ensures that the TOE enforces the PrivUserAccess SFP so that only system administrators have the capability to query, modify, delete, create, or install specified security attributes, keys and certificates, and IPv4 filter rules. |
| O.PROTECT_COM | 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.<br><br>FCS_CKM.1 (all but UDE), FCS_CKM.2 (all), FCS_CKM.4, and FCS_COP.1 (all but UDE) ensure that the TOE provides the cryptographic support and services and associated key management capabilities necessary to assure secure communication between TOE components and remote trusted products (incoming and outgoing) by using specified cryptographic key generation algorithms and associated cryptographic key distribution and destruction methods.<br><br>FDP_IFC.1 (IPSEC, SSL and SNMP), FDP_IFF.1 (IPSEC, SSL and SNMP), FDP_UCT.1 (IPSEC, SSL and SNMP), and FDP_UIT.1 (IPSEC, SSL and SNMP), SSLSec SFP, SNMPSec SFP and IP Security SFP are enforced to |

| | |
|---|---|
| | control and protect information flow between controlled subjects (IPv4 address, destination port, etc.) based on specific subject and information security attributes to enable the transmission and receipt of user data in a protected manner.<br><br>FMT_SMF.1 requires that there is a possibility to invoke the SSL, IP Filtering, IPSec and SNMPv3 functions. FMT_MOF.1 (FMT 1) specifies that these functions can be enabled or disabled by the system administrator. FMT_MOF.1 (FMT 2) restricts the use of these functions to the system administrator. FMT_SMR.1 manages the role "system administrator".<br><br>FTP_ITC.1 and FTP_TRP.1 (all) 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.<br><br>FPT_STM.1 ensures that the TOE provides a reliable timestamp for inclusion in cryptographic operations.<br><br>FMT_MTD.1 (SNMP) ensures that the TOE enforces the SNMPSec SFP so that only system administrators have the capability to query, modify, delete, create, or install specified security attributes, keys and passwords, and SNMP configuration information. |
| O.PROTECT_DAT | FCS_CKM.4, FCS_CKM.1 (UDE) and FCS_COP.1 (UDE) ensure that the TOE provides the cryptographic support and services and associated key management capabilities necessary to assure data protection for stored files by using specified cryptographic key generation algorithms and associated cryptographic key distribution and destruction methods.<br><br>FDP_RIP.1 (IOW 1) and FDP_RIP.1 (IOW2) protect data by ensuring that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing.<br><br>FDP_RIP.1 (IOW 3) protects data by ensuring that stored document data and directory information does not remain on the mass storage device once the system administrator has determined that the stored jobs and data are no longer necessary. |

## 5.8. Rationale for Security Assurance Requirements

This ST has been developed for multi-function digital image processing products incorporating Image Overwrite Security function, an Authentication and Authorization function, an Audit

Logging function, an IP Filtering function, and cryptographic network communications protocols. The TOE environment will be exposed to only a low level of risk because the TOE sits in office space where it is under almost constant supervision. Agents cannot physically access the HDD or FAX without disassembling the TOE. Agents have no means of infiltrating the TOE with code to effect a change. As such, the Evaluation Assurance Level 2 is appropriate.

That Assurance Level is augmented with ALC_FLR.3, Systematic flaw remediation. ALC_FLR.3 ensures that instructions and procedures for the reporting, configuration management, and remediation of identified security flaws are in place and their inclusion is expected by the consumers of this TOE.

# 5.9. Rationale for Dependencies

## 5.9.1. Security Functional Requirement Dependencies

Table 12 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

**Table 12: 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 (SSL 1) | FCS_CKM.2 or FCS_COP.1 | Yes, FCS_CKM.2 (SSL 1) and FCS_COP.1 (SSL 2) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.1 (SSL 2) | FCS_CKM.2 or FCS_COP.1 | Yes, FCS_CKM.2 (SSL 2) and FCS_COP.1 (SSL1) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.1 (IPSEC) | FCS_CKM.2 or FCS_COP.1 | Yes, FCS_COP.1 (IPSEC 1) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.1 (SNMP) | FCS_CKM.2 or FCS_COP.1 | Yes, FCS_COP.1 (SNMP) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.2 (SSL 1) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (SSL 1) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.2 (SSL 2) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (SSL 2) |

| Functional Component ID | Dependency (ies) | Satisfied |
|---|---|---|
| | FCS_CKM.4 | Yes |
| FCS_CKM.1(UDE) | FCS_CKM.2 or FCS_COP.1 | Yes, FCS_COP.1 (UDE) |
| | FCS_CKM.4 | Yes |
| FCS_CKM.4 | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (ALL) |
| FCS_COP.1 (IPSEC 1) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (IPSEC) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (IPSEC 2) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (IPSEC) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (IPSEC 3) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (IPSEC) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (SNMP) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (SNMP) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (SSL 1) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (SSL 2) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (SSL 2) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (SSL 1) |
| | FCS_CKM.4 | Yes |
| FCS_COP.1 (UDE) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Yes, FCS_CKM.1 (UDE) |
| | FCS_CKM.4 | Yes |
| FDP_ACC.1 | FDP_ACF.1 | Yes |
| FDP_ACF.1 | FDP_ACC.1 | Yes |
| | FMT_MSA.3 | No[3] |

[3] The dependency of FDP_ACF.1 and FDP_IFF.1 (FILTER, IPSEC, SSL and SNMP) on FMT_MSA.3 is not met because none of these functions support "a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values." (CC Part 3 Page 106). The TOE does not give system administrators the option of specifying default values, permissive or otherwise. In fact, these features are configured

| Functional Component ID | Dependency (ies) | Satisfied |
|---|---|---|
| FDP_IFC.1 (IOW) | FDP_IFF.1 | Yes, FDP_IFF.1 (IOW) |
| FDP_IFF.1 (IOW) | FDP_IFC.1 | Yes, FDP_IFC.1 (IOW) |
| | FMT_MSA.3 | Yes, FMT_MSA.3 (IOW) |
| FDP_IFC.1 (FLOW) | FDP_IFF.1 | Yes, FDP_IFF.1 (FLOW) |
| FDP_IFF.1 (FLOW) | FDP_IFC.1 | Yes, FDP_IFC.1 (FLOW) |
| | FMT_MSA.3 | Yes, FMT_MSA.3 (FLOW) |
| FDP_IFC.1 (FILTER) | FDP_IFF.1 | Yes, FDP_IFF.1 (FILTER) |
| FDP_IFF.1 (FILTER) | FDP_IFC.1 | Yes, FDP_IFC.1 (FILTER) |
| | FMT_MSA.3 | No[3] |
| FDP_IFC.1 (IPSEC) | FDP_IFF.1 | Yes, FDP_IFF.1 (IPSEC) |
| FDP_IFF.1 (IPSEC) | FDP_IFC.1 | Yes, FDP_IFC.1 (IPSEC) |
| | FMT_MSA.3 | No[3] |
| FDP_IFC.1 (SSL) | FDP_IFF.1 | Yes, FDP_IFF.1 (SSL) |
| FDP_IFF.1 (SSL) | FDP_IFC.1 | Yes, FDP_IFC.1 (SSL) |
| | FMT_MSA.3 | No[3] |
| FDP_IFC.1 (SNMP) | FDP_IFF.1 | Yes, FDP_IFF.1 (SNMP) |
| FDP_IFF.1 (SNMP) | FDP_IFC.1 | Yes, FDP_IFC.1 (SNMP) |
| | FMT_MSA.3 | No[3] |
| FDP_RIP.1 (IOW 1) | None | |
| FDP_RIP.1 (IOW 2) | None | |
| FDP_RIP.1 (IOW 3) | None | |
| FDP_UCT.1 (IPSEC) | FDP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (IPSEC) |
| | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (IPSEC) |
| FDP_UCT.1 (SSL) | FTP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (SSL) |
| | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (SSL) |
| FDP_UCT.1 (SNMP) | FTP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (SNMP) |

and, with the exception of IP Filter rules, cannot be modified by the system administrator other than to enable or disable them. It is for these reasons that the dependency on FMT_MSA.3 is not and cannot be expected to be met.

| Functional Component ID | Dependency (ies) | Satisfied |
|---|---|---|
| | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (SNMP) |
| FDP_UIT.1 (IPSEC) | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (IPSEC) |
| | FTP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (IPSEC) |
| FDP_UIT.1 (SSL) | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (SSL) |
| | FTP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (SSL) |
| FDP_UIT.1 (SNMP) | FDP_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (SNMP) |
| | FTP_ITC.1 or FTP_TRP.1 | Yes, FTP_TRP.1 (SNMP) |
| FIA_AFL.1 (AUT 1) | FIA_UAU.1 | Yes, hierarchically by FIA_UAU.2 |
| FIA_AFL.1 (AUT 2) | FIA_UAU.1 | Yes, hierarchically by FIA_UAU.2 |
| FIA_UAU.2 | FIA_UID.1 | Yes, hierarchically by FIA_UID.2. Identification of the system administrator at the Local User Interface is implicit -- the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window. |
| FIA_UAU.7 | FIA_UAU.1 | Yes, hierarchically by FIA_UAU.2 |
| FIA_UID.2 | None | |
| FMT_MOF.1 (FMT 1) | FMT_SMF.1 | Yes |
| | FMT_SMR.1 | Yes |
| FMT_MOF.1 (FMT 2) | FMT_SMF.1 | Yes |
| | FMT_SMR.1 | Yes |
| FMT_MSA.1 (IOW) | FMT_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (IOW) |
| | FMT_SMR.1 | 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.1 (FLOW) | FMT_ACC.1 or FDP_IFC.1 | Yes, FDP_IFC.1 (FLOW) |
| | FMT_SMR.1 | No, because the authorized identified roles allowed to |

| Functional Component ID | Dependency (ies) | Satisfied |
|---|---|---|
| | | 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 (IOW) | FMT_MSA.1 | Yes, FMT_MSA.1 (IOW) |
| | 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.3 (FLOW) | FMT_MSA.1 | Yes, FMT_MSA.1 (FLOW) |
| | 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_MTD.1 (AUT) | FMT_SMF.1 | Yes |
| | FMT_SMR.1 | Yes |
| FMT_MTD.1 (FILTER) | FMT_SMF.1 | Yes |
| | FMT_SMR.1 | Yes |
| FMT_MTD.1 (SNMP) | FMT_SMF.1 | Yes |
| | FMT_SMR.1 | Yes |
| 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. |
| FPT_STM.1 | None | |
| FTP_ITC.1 | None | |
| FTP_TRP.1 (IPSEC) | None | |
| FTP_TRP.1 (SSL) | None | |
| FTP_TRP.1 (SNMP) | None | |

## 5.9.2. Security Assurance Requirement Dependencies

SAR dependencies identified in the CC have been met by this ST as shown in Table 13.

**Table 13: EAL2 (Augmented with ALC_FLR.3) SAR Dependencies Satisfied**

| Assurance Component ID | Dependencies | Satisfied |
|---|---|---|
| ADV_ARC.1 | ADV_FSP.1,<br>ADV_TDS.1 | Yes |
| ADV_FSP.2 | ADV_TDS.1 | Yes |
| ADV_TDS.1 | ADV_FSP.2 | Yes |
| AGD_OPE.1 | ADV_FSP.1 | Yes |
| AGD_PRE.1 | None | |
| ALC_CMC.2 | ALC_CMS.1 | Yes |
| ALC_CMS.2 | None | |
| ALC_DEL.1 | None | |
| ALC_FLR.3 | None | |
| ASE_CCL.1 | ASE_ECD.1<br>ASE_INT.1<br>ASE_REQ.1 | Yes<br>Yes<br>Yes |
| ASE_ECD.1 | None | |
| ASE_INT.1 | None | |
| ASE_OBJ.2 | ASE_SPD.1 | Yes |
| ASE_REQ.2 | ASE_ECD.1<br>ASE_OBJ.2 | Yes<br>Yes |
| ASE_SPD.1 | None | |
| ASE_TSS.1 | ASE_ARC.1<br>ASE_INT.1<br>ASE_REQ.1 | Yes<br>Yes<br>Yes |
| ATE_COV.1 | ADV_FSP.2<br>ATE_FUN.1 | Yes<br>Yes |
| ATE_FUN.1 | ATE_COV.1 | Yes |
| ATE_IND.2 | ADV_FSP.2<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_COV.1<br>ATE_FUN.1 | Yes<br>Yes<br>Yes<br>Yes<br>Yes |
| AVA_VAN.2 | ADV_ARC.1<br>ADV_FSP.1<br>ADV_TDS.1<br>AGD_OPE.1<br>AGD_PRE.1 | Yes<br>Yes<br>Yes<br>Yes<br>Yes |

# 6. TOE SUMMARY SPECIFICATION

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

## 6.1. TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1.

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

### 6.1.1. Image Overwrite (TSF_IOW)

**FDP_RIP.1 (IOW 1), FDP_RIP.1 (IOW 2), FDP_RIP.1 (IOW 3), FDP_IFC.1 (IOW), FDP_IFF.1 (IOW), FMT_MSA.1 (IOW, FMT_MSA.3 (IOW)**

The TOE implements an image overwrite security function to overwrite temporary files created during the printing, network scan, or scan to email, and LanFax process.

The network controller spools and processes documents to be printed or scanned. Temporary files are created as a result of this processing on a reserved section of the hard disk drive of the network controller. The definition of this reserved section is statically stored within the TOE and cannot be manipulated. Immediately after the job has completed, the files are overwritten using a three pass overwrite procedure as described in DOD 5200.28-M.

User image files associated with the Copy/Print, Store and Reprint feature may be stored long term for later reprinting. When a job is selected for reprint, the stored job is resubmitted to the system. Temporary files created during processing are overwritten at the completion of the job

using the 5200.28-M algorithm. The stored jobs are not overwritten until the jobs are deleted by the user, or when the System Administrator executes a full on-demand image overwrite. A standard on-demand image overwrite (ODIO) overwrites all files written to temporary storage areas of the HDD and the temporary storage area of the Fax card flash memory. A full ODIO overwrites those files as well as the Fax mailbox/dial directory (in Fax card flash memory), Scan to mailbox data, and all files that have been stored at the request of a user via Copy/Print, Store and Reprint jobs.

The embedded fax card buffers incoming and outgoing fax images in flash memory. Immediately after an embedded fax job has completed, the files are overwritten using a single-pass zeroization method. The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M.

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, overwrites the contents of the embedded fax card flash memory using a single-pass zeroization method, and then the network controller reboots. The embedded fax card flash memory overwrite is not compliant with DoD 5200.28-M. A scheduling function allows ODIO to be executed on recurring basis as set up by the System Administrator.

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 ODIO was started from the Web Interface, it cannot be aborted from either the WebUI or Local UI.

If the TOE is turned back on after a power failure, the TOE automatically starts an IIO procedure for all abnormally terminated print or scan jobs stored on the HDD and on the fax card flash memory prior to coming “on line”.

### 6.1.2. Information Flow Security (TSF_FLOW)

**FDP_IFC.1 (FLOW), FDP_IFF.1 (FLOW), FMT_MSA.1 (FLOW), FMT_MSA.3 (FLOW)**

The TOE provides separation between the optional FAX processing board and the network controller and prevents therefore an interconnection between the PSTN and the internal network as illustrated in Figure 2.

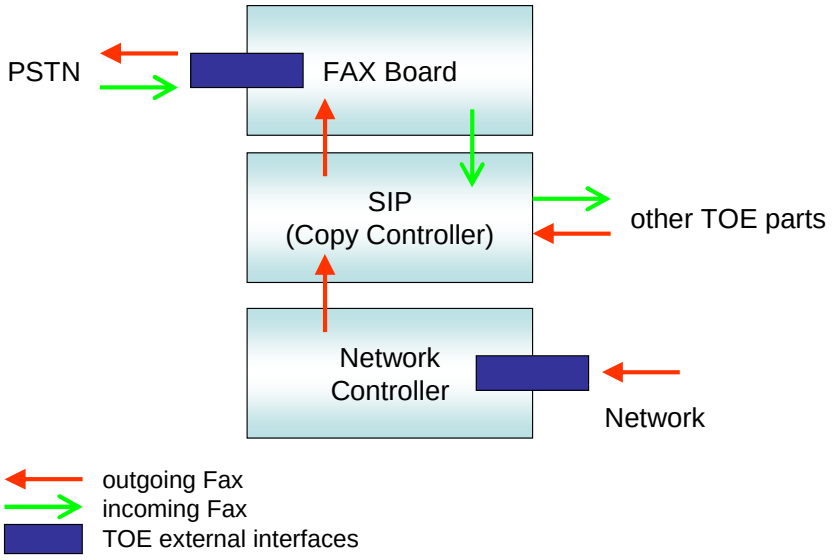


Figure 2: TSF_FLOW

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

For outgoing FAX the copy controller will push image data to the FAX card. The image data can come from the network controller or another part of the TOE (e.g., the optical scanner). The copy controller will inform the FAX card when it has finished the transfer of the image data. The FAX card cannot access the shared memory area until the copy controller has completed its transfer of outgoing FAX image data. Likewise the copy controller cannot access the shared memory area until the FAX card has completed its transfer of incoming FAX image data.

For incoming FAX the FAX card will inform the copy controller when there is a FAX available for collection after the transmission of the fax has finished and the PSTN connection is terminated. The copy controller will pull image data from the FAX card. The copy controller sends the image data only to the IOT software, which prints the FAX to paper.

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

### 6.1.3. Authentication (TSF_ AUT)

**FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_AFL.1 (AUT 1), FIA_AFL.1 (AUT 2), FMT_SMR.1**

The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions (see 6.1.11). 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 explicit -- the

administrator will identify themselves by entering the username "admin" in the authentication window. Identification of the system administrator at the Web user Interface is explicit -- the administrator will identify themselves by entering the username "admin" in the authentication dialog window.

The authentication process will be delayed at the Local User Interface, for at least 3 minutes if 3 wrong PINs were entered in succession. If 3 wrong PINs are entered at the web interface, the TOE will lock out the SA login function at the Web User Interface for a period of 5 minutes.

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

The Web user interface can be configured such that authentication of the system administrator is based upon individual credentials. If configured for local authentication the system requires the system administrator to enter a username and password. The system will authenticate the user against an internal database. Alternatively the system may be configured such that authentication is performed remotely by the network's domain controller. In this case, the SA must enter a valid fully-qualified username and password. In both cases, privileged user status is granted based upon successful authentication.

### 6.1.4. Network Identification (TSF_NET_ID)

**FIA_UAU.2, FIA_UID.2**

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and Embedded Fax); 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: CAC two-factor local authentication, LDAP v4, Kerberos (Solaris), Kerberos (Windows 2000/2003), NDS (Novell 4.x, 5.x), 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. Also note, in CAC two-factor local authentication mode, the user's certificate on the card is not currently checked for validity (using OCSP).

### 6.1.5. Security Audit (TSF_FAU)

**FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FMT_MTD.1 (AUT), FTP_STM.1**

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, and LanFax jobs. Copy jobs are not tracked. By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for

transmission of data outside of the local environment, as required by such legislation as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc.

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

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

The Guidance documentation defines only one user authentication method: *Network Authentication* (see Section 6.1.3 above). *Network Authentication* is mutually exclusive with *Auditron* and *XSA*,, however, it can be enabled concurrently with *Network Accounting*.

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

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

If *Network Authentication* is enabled, then the name required by *Network Authentication* will be recorded in the audit log.

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

### 6.1.6. Cryptographic Support (TSF_FCS)

**FCS_CKM.1 (All), FCS_CKM.4, FCS_COP.1 (All)**

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

### 6.1.7. User Data Protection – SSL (TSF_FDP_SSL)

**FCS_CKM.1 (SSL 1), FCS_CKM.1 (SSL 2), FCS_CKM.2 (SSL 1), FCS_CKM.2 (SSL 2), FCS_COP.1 (SSL 1), FCS_COP.1 (SSL 2), FDP_IFC.1 (SSL), FDP_IFF.1 (SSL), FDP_UCT.1 (SSL), FDP_UIT.1 (SSL), FTP_ITC.1, FTP_TRP.1 (SSL)**

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE

is performing. SSL must be enabled before setting up either IPSec, SNMPv3, or before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. 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. The TOE creates and enforces the informal security policy model, "All communications to the Web server will utilize SSL (HTTPS)."

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

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

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

### 6.1.8. User Data Protection – IP Filtering (TSF_FDP_FILTER)

**FDP_IFC.1 (FILTER), FDP_IFF.1 (FILTER), FMT_MTD.1 (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" IPv4 packets. These rules include a listing of IPv4 addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

**Note: The TOE cannot enforce the IP Filtering (TSF_FDP_FILTER) security function when it is configured for IPv6, AppleTalk or IPX networks.**

### 6.1.9. User Data Protection – IPSec (TSF_FDP_IPSec)

**FCS_CKM.1 (IPSEC), FCS_COP.1 (IPSEC 1), FCS_COP.1 (IPSEC 2), FCS_COP.1 (IPSEC 3), FDP_IFC.1 (IPSEC), FDP_IFF.1 (IPSEC), FDP_UCT.1 (IPSEC), FDP_UIT.1 (IPSEC), FTP_TRP.1 (IPSEC)**

The TOE implements the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE through the lpr and port 9100 network interfaces. Printing clients initiate the establishment of a security association with the MFD. The MFD establishes a security association with the printing client using IPSec "tunnel mode." Thereafter, all IPv4-based traffic to and from this destination will pass through the IPSec tunnel

until either end powers down, or resets, after which the tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client.

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

**Note: The TOE cannot enforce the IPSec (TSF_FDP_IPSec) security function when it is configured for IPv6, AppleTalk or IPX networks.**

### 6.1.10. Network Management Security (TSF_NET_MGMT)

**FCS_CKM.1 (SNMP), FCS_COP.1 (SNMP), FDP_IFC.1 (SNMP), FDP_IFF.1 (SNMP), FDP_UCT.1 (SNMP), FDP_UIT.1 (SNMP), FMT_MTD.1 (SNMP), FTP_TRP.1 (SNMP)**

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

As implemented, both an authentication and privacy (encryption) password must be set up both at the device and at the manager. Both passwords must be a minimum of 8 characters. SNMP uses MD5 for authentication and single-DES in Cipher Block Chaining mode for encryption. SNMPv3 utilizes the OpenSSL crypto library for the authentication and encryption functions.

### 6.1.11. Security Management (TSF_FMT)

**FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_MOF.1 (FMT 1), FMT_MOF.1 (FMT 2)**

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

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

Additionally, only authenticated system administrators can assign authorization privileges to users, establish a recurrence schedule for “On Demand” image overwrite, enable/disable SSL support, enable/disable and configure IPSec tunneling, enable/disable and configure SNMPv3, create/install X.509 certificates, enable/disable and download the audit log, enable/disable and configure (rules) IP filtering, or enable/disable and configure IPv6.

### 6.1.12. User Data Protection - AES (TSF_EXP_UDE)

**FCS_CKM.1 (UDE), FCS_COP.1 (UDE))**

The TOE utilizes data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, to support encryption and decryption of designated portions of the hard disk where user files may be stored.

Those packages include provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-128-FIPS-197.

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

# 7. ACRONYMS

The following acronyms are used in this Security Target:

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

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