Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040, and M9050 with Jetdirect Inside Firmware Security Target

Certification ID: BSI-DSZ-CC-0566

Version: 2.2

Last Update: 2013-10-23

Trademarks

atsec is a trademark of atsec GmbH

IEEE is a registered trademark in the U.S. patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

Java and all Java-based products are trademarks of Oracle Corporation, in the United States, other countries, or both.

2600.2 is a trademark of The Institute of Electrical and Electronics Engineers, Incorporated.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Table of Content

Document History

Version	Date	Changes	Author
2.2	2013-10-23	HP MFP firmware ST.	Scott Chapman, atsec

References

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-2007-09-001 to CCIMB-2007-09-003, Version 3.1 Revision 2, September 2007, Part 1 to 3

[CCEVS-PL20] NIAP CCEVS Policy Letter #20, November 11, 2010

[2600.2] IEEE Std 2600.2™-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™-2008 Operational Environment B with NIAP CCEVS Policy Letter #20

1 ST Introduction

This security target documents the security characteristics of the Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040, and M9050 with Jetdirect Inside firmware (where MFP is an abbreviation for Multifunction Product). The TOE is the HCD System Firmware (a.k.a. MFP Firmware) and the Jetdirect Inside Firmware described later in this chapter. The hardware is part of the operational environment. This security target includes the use of the IEEE Std 2600.2™-2009 protection profile for hardcopy devices (HCDs) with NIAP CCEVS Policy Letter #20.

1.1 ST Structure

The structure of this document is as defined by [CC] Part 1 Annex A.

- Section 1 is the ST Introduction.
- Section 2 provides the Conformance Claims.
- Section 3 provides the Security Problem Definition
- Section 4 provides the Security Objectives
- Section 5 provides the Extended Components Definition
- Section 6 provides the Security Requirements
- Section 7 provides the TOE Summary Specifications

1.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrative User: This term refers to a user with administrative control of an HCD.

Authentication Data: This includes the PIN and/or password for each user of the product.

External Interface: A non-hardcopy interface where either the input is being received from outside the TOE or the output is delivered to a destination outside the TOE.

Hardcopy Device (HCD): This term generically refers to the product models in this security target.

Shared-medium Interface: Mechanism for transmitting or receiving data that uses wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users.

User Security Attributes: Defined by functional requirement FIA_ATD.1, every user is associated with one or more security attributes which allow the TOE to enforce its security functions on this user.

1.3 ST Reference and TOE Reference

ST Title	Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040, and M9050 with Jetdirect Inside Firmware Security Target
ST Version	2.2
ST Publication Date	2013-10-23
Sponsor	Hewlett-Packard Development Company, L.P.
Developer	Hewlett-Packard Development Company, L.P.
Certification ID	BSI-DSZ-CC-0566
Keywords	Hewlett-Packard, HP, Color LaserJet, LaserJet, CM6040, CM6030, M9050S, M9040, multifunction product, MFP, hardcopy device, HCD, Printer, Jetdirect Inside, Secure File Erase, Secure Storage Erase, separation of analog fax from network.
TOE Reference	• HP Color LaserJet CM3530 MFP and CM3530fs MFP* o MFP Firmware version: 20130128 53.194.1

	o Jetdirect Inside version: V.43.16.FF • HP Color LaserJet CM6030 MFP and CM6030f MFP* o MFP Firmware version: 20130128 52.215.5 o Jetdirect Inside version: V.43.16.FF • HP Color LaserJet CM6040 MFP and CM6040f MFP* o MFP Firmware version: 20130128 52.215.5 o Jetdirect Inside version: V.43.16.FF • HP LaserJet M9040 MFP* o MFP Firmware version: 20130128 51.214.5 o Jetdirect Inside version: V.43.16.FF • HP LaserJet M9050 MFP* o MFP Firmware version: 20130128 51.214.5 o Jetdirect Inside version: V.43.16.FF * The hardware is part of the operational environment.

All MFP Firmware versions above contain LynxOS version 4.0.0b.

1.4 TOE Overview

The TOE is the firmware inside of the Hewlett-Packard LaserJet MFPs, which are enterprise network multifunction products designed to be shared by many client computers and users. The TOE is designed to meet the requirements of [2600.2] in the environment defined by [2600.2]. It provides the functions for the copying, faxing, printing, and scanning of documents. These hardcopy devices (HCDs), as they are called in [2600.2], are self-contained units that include a processor, memory, networking, hard drive, scanner, and print engine as well as the TOE.

The HCD models used in the evaluation are listed in section 1.3 under TOE Reference along with the evaluated firmware version numbers for each model. The TOE provides the following security features:

- Auditing
- Identification and Authentication
- Data Protection and Access Control
- Protection of the TSF (restricted forwarding, TSF self-testing, timestamps)
- TOE Access Protection (inactivity timeout)
- Trusted Channel Communication
- Management

1.4.1 Intended Method of Use

[2600.2] is defined for a commercial information processing environment in which a moderate level of document security, network security, and security assurance, are required.

The TOE is intended to be used in non-hostile, networked environment where TOE users have direct physical access to the HCD for copying, faxing, printing, and scanning. The physical environment should be reasonably controlled and/or monitored where physical tampering of the HCD and/or the TOE would be evident and noticed.

The TOE can be connected to multiple client computers via a local area network using HP's Jetdirect Inside in the evaluated configuration. The evaluated configuration uses secure network mechanisms for communication between the network computers and the TOE. The TOE is not intended be connected to the Internet.

Analog fax phone lines can be connected to the TOE in the evaluated configuration for sending and receiving faxes.

The evaluated configuration contains a built-in user identification and authentication database that is part of the TOE and it also supports external/remote Kerberos and LDAP authentication servers to identify and authenticate users.

The evaluated configuration supports the HP Web Jetadmin administrative application for managing the TOE. This application uses HTTP, SNMP, and PJL to communicate to the TOE. (The Web Jetadmin application is part of the operational environment, not the TOE.) The evaluated configuration also supports the Embedded Web Server (EWS) interface for managing the TOE using a web browser over HTTP. (Web browsers are part of the operational environment, not the TOE.)

In addition, the evaluated configuration supports remote file systems for storing scanned documents remotely.

1.5 TOE Description

1.5.1 TOE Architecture

As mentioned previously, the TOE is the HCD System Firmware (a.k.a. MFP Firmware) and Jetdirect Inside Firmware inside an enterprise network multifunction product that is designed to be shared by many client computers and human users. It performs the functions of copying, faxing, printing, and scanning of documents. It can be connected to a local network through the HP Jetdirect Inside built-in Ethernet and to an analog phone line using its internal analog fax modem.

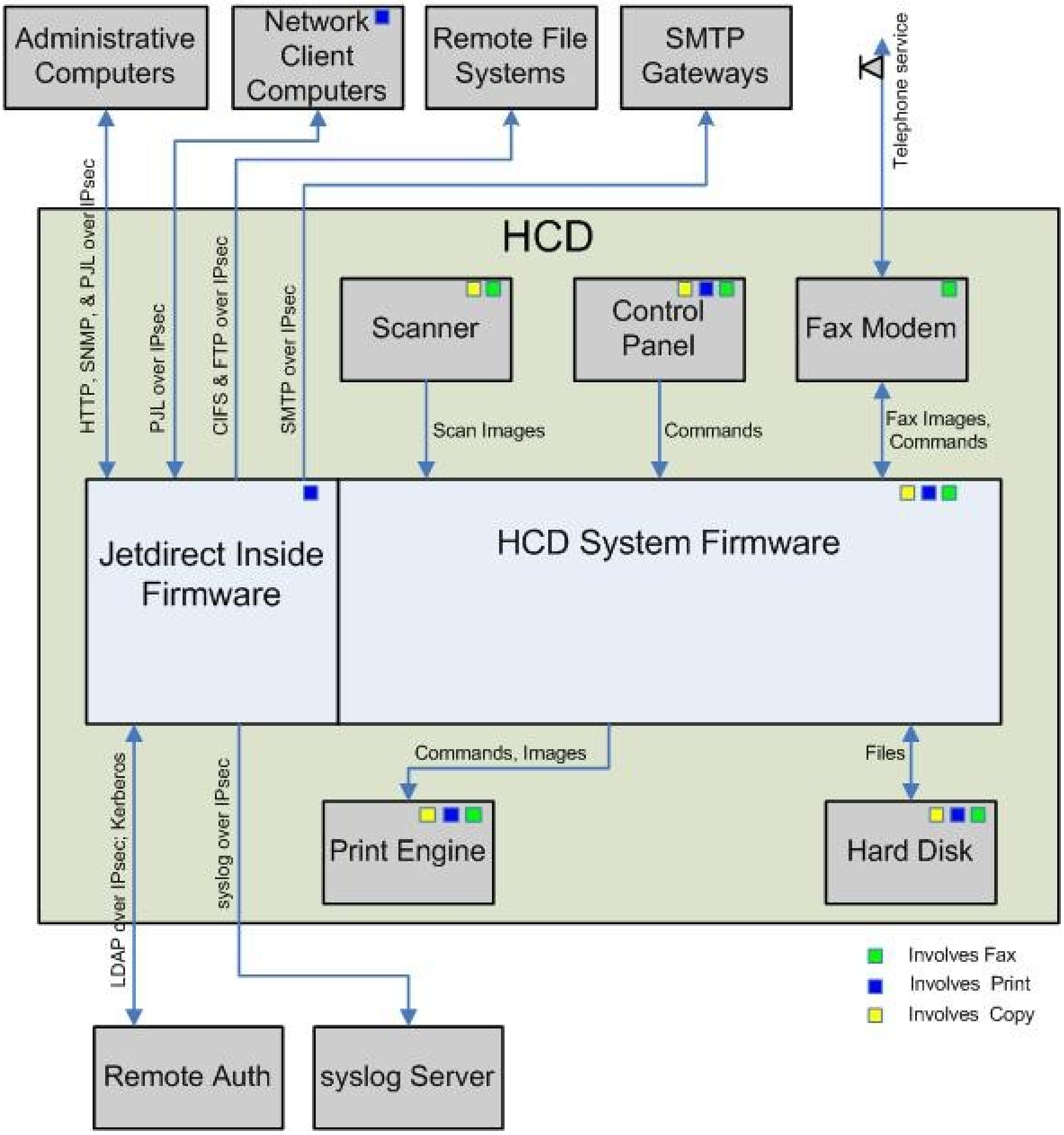

Figure 1-1- HCD physical diagram

Figure 1-1 shows a high-level physical diagram of an HCD.

At the top of this figure are the Administrative Computers. Administrative Computers connect to the TOE using IPsec with X.509v3 certificates for both mutual authentication and for protection of data from disclosure and alteration. These computers can administer the TOE using the EWS, SNMP, and Printer Job Language (PJL) interfaces. The HTTP-based EWS administrative interface allows administrators to remotely manage the features of the TOE using a web browser. The same EWS HTTP interface also supports the Digital Sender Module Protocol (DSMP), used to read and write XML-based device objects, and the HTTP-based certificate uploading of X.509v3 certificates. The SNMP interface allows administrators to remotely manage the TOE using SNMP-based administrative applications like the HP Web Jetadmin application. The PJL interface allows administrators to manage protected data by password protecting administrative data with the PJL Password. (Remote applications such as web browsers and Web Jetadmin are part of the operational environment, not part of the TOE.)

Since IPsec authenticates the computers (i.e. IPsec authenticates the computer itself; IPsec does not authenticate the individual users of the computer), access to the Administrative Computers should be restricted to TOE administrators only. (The PJL interface requires the user to know the current PJL Password in order to change protected values.)

The TOE distinguishes between Administrative Computers and Network Client Computers by using IP addresses and the IPsec/Firewall. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one.

The evaluated configuration supports the following SNMP versions:

- SNMPv1 read-only
- SNMPv2c read-only
- SNMPv3

Network Client Computers connect to the TOE using IPsec with X.509v3 certificates to protect the communication and to mutually authenticate. These client computers can send print jobs to the TOE using the PJL interface as well as receive job status.

The TOE supports an optional analog telephone line connection for sending and receiving faxes. The Control Panel uses identification and authentication to control access for sending analog faxes. Since the fax protocol doesn't support authentication of incoming analog fax phone line users, anyone can connect to the analog fax phone line, but the only function an incoming fax phone line user can perform is to transmit a fax to the TOE.

The TOE also supports remote file systems for the storing of scanned documents. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate. The TOE supports the File Transfer Protocol (FTP) and the Common Internet File System (CIFS) protocol for remote file system connectivity.

The TOE can be used to email scanned documents. The TOE supports protected communications between the TOE and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutual authenticate with the SMTP gateway. The TOE can only protect the email up to the SMTP gateway. It is the responsibility of the operational environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

Remote authentication servers can be used with the TOE. The TOE supports both LDAP and Kerberos. The TOE uses IPsec with X.509v3 certificates to protect LDAP communications. It uses the Kerberos protocol for protecting Kerberos communications.

Each HCD contains a user interface called the Control Panel that is controlled by the TOE. The Control Panel consists of a touch sensitive LCD screen and several physical buttons that are attached to the HCD. It is the interface device that a user uses to communicate to the TOE when physically using the HCD. The LCD screen displays information such as menus and status to the user. It also provides virtual buttons to the user such as an alphanumeric keypad for entering usernames and passwords.

The Scanner is the part of the HCD that converts hardcopy documents into electronic format. The Print Engine converts electronic format into hardcopy.

The Hard Disk (a.k.a. hard drive) provides persistent storage for documents. The hard drive contains a section called Job Storage which is a user-visible file system where stored jobs such as certain types of fax jobs, certain types of print jobs, and certain types of copy jobs are stored/held until deleted/released by a user, or depending on the job type, stored until the HCD is rebooted if no user action is taken.

The TOE supports the auditing of security relevant functions. It contains an internal fixed-size audit log file for storing audit events and also forwards the audit events to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between the TOE and the syslog server and to mutually authenticate the TOE and syslog server.

The Jetdirect Inside Firmware and HCD System Firmware components comprise the firmware on the system. Though they are shown as two separate components, they both run in the same instance of the operating system. Both firmware components contain an Embedded Web Server (EWS). The two firmware components communicate with each other through these two web servers.

The Jetdirect Inside firmware includes SNMP, IPsec/Firewall, and the management functions for managing these network-related features. The Jetdirect Inside firmware also controls the HCD's Ethernet network interface.

The HCD System Firmware controls the other functions of the TOE not controlled by Jetdirect Inside (from the Control Panel to the hard drive to the print jobs).

Table 1-1 shows the main TOE functions available to a normal user (defined as U.NORMAL in [2600.2]) and the terminology used in the TOE's guidance documentation.

Table 1-1 - HCD terminology for user functions

	Input From					**Output To**							
Function	Scanner	Network Client Computer	Phone Line	Job Storage (non-fax)	Job Storage (fax only)	Hard Copy	Job Storage (non-fax)	Job Storage (fax only)	Phone Line	Email (SMTP)	File Server	FTP	**HP LaserJet Terminology**
Scan	X						X						Stored Copy Job
	X									X			Send E-mail
	X										X		Send to Folder
	X											X	Send to Folder
Copy	X					X							Copy Job, Color Copy Job
Print		X				X	X						Quick Print, Proof and Hold, Normal (Job Storage Mode off)
		X					X						Stored Job, Personal Print Job, Private Job
				X		X							Print from Job Storage (Job PIN may be required)
					X	X							Print Fax (Fax PIN required)
Fax In			X					X					Receive Fax
			X			X							Fax Polling Receive
			X							X			Archive to Email Address
Fax Out	X								X				Send Fax, Archive to Fax Number
	X									X			Archive to Email Address

Figure 1-2 shows the TOE boundary (i.e. the HCD System Firmware (a.k.a. MFP Firmware) and the Jetdirect Inside Firmware) in blue. The Jetdirect Inside Firmware contains the network connectivity firmware such as the network device drivers and network infrastructure, which plugs into the HCD System Firmware. The HCD System Firmware contains the bootloader used to bootload the operating system, the operating system, and applications that drive the functions of the TOE. Both components work together to provide the security functionality defined in this document for the TOE. (PSTN is an abbreviation for Public Switched Telephone Network.)

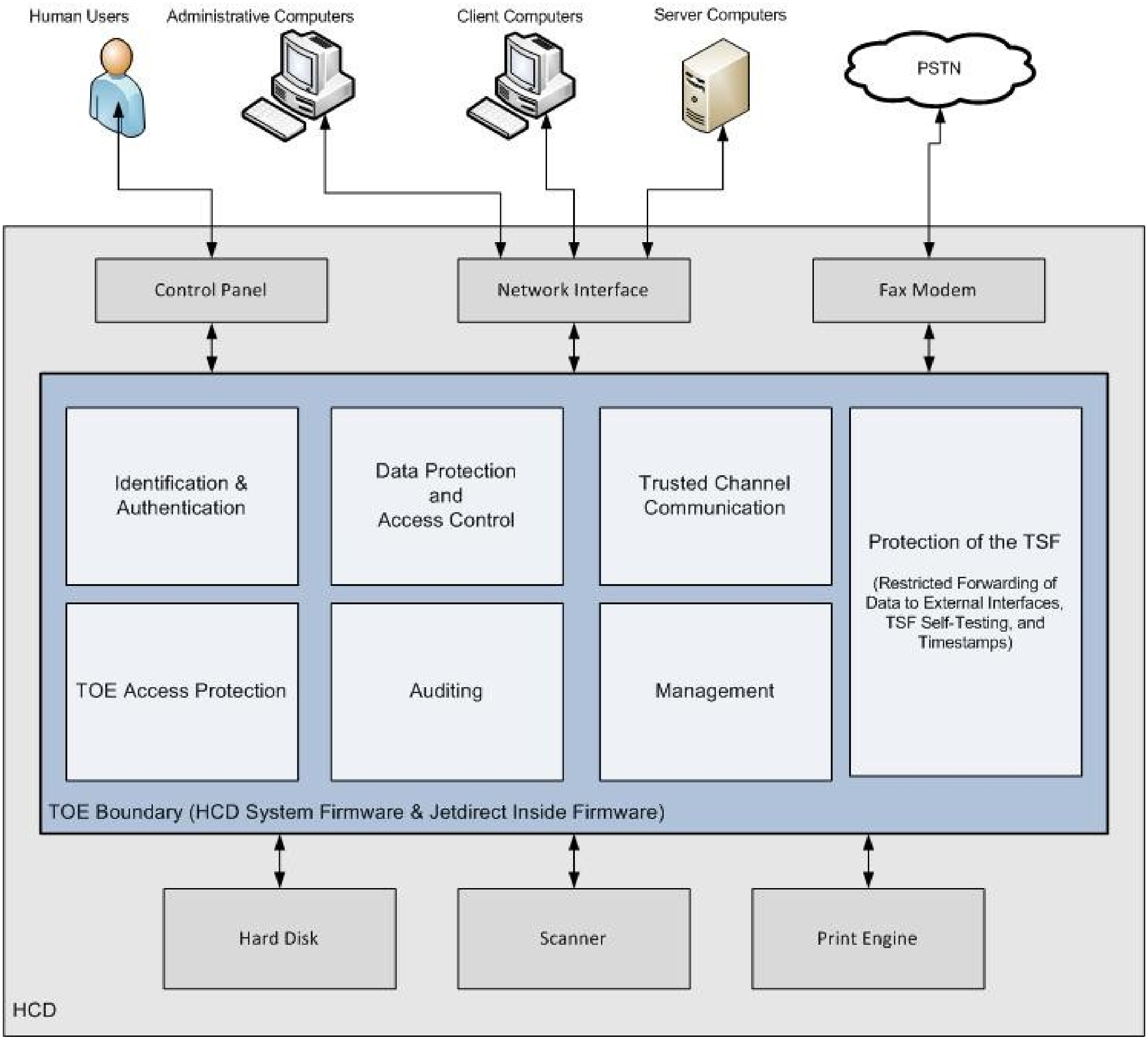
Human Users
Administrative Computers
Client Computers
Server Computers
PSTN
Control Panel
Network Interface
Fax Modem
Identification & Authentication
Data Protection and Access Control
Trusted Channel Communication
Protection of the TSF
(Restricted Forwarding of Data to External Interfaces, TSF Self-Testing, and Timestamps)
TOE Access Protection
Auditing
Management
TOE Boundary (HCD System Firmware & Jetdirect Inside Firmware)
Hard Disk
Scanner
Print Engine
HCD

Figure 1-2: HCD logical diagram.

1.5.2 TOE Security Function (TSF) Summary

1.5.2.1 Auditing

The TOE performs auditing of security relevant functions. The TOE maintains an internal, fixed-size audit log file for storage of audited records and protects the log from non-administrative access. The TOE also connects and sends records to a syslog server for long-term storage and audit review. (The syslog server is part of the operational environment.)

1.5.2.2 Identification & Authentication

1.5.2.2.1 Control Panel I&A

All HCDs have a Control Panel controlled by the TOE and used for selecting a function to be performed, such as Print, Copy, Scan, and Fax. The TOE supports both local and remote authentication via the Control Panel. The local authentication mechanism is called User PIN Authentication which identifies and authenticates users based on a unique Personal Identification Number (PIN). The supported remote authentication mechanisms are Kerberos and LDAP. For these remote mechanisms, Control Panel users must enter their username and password as defined by these remote mechanisms.

The Control Panel also supports two modes of operation called Walk Up Authentication mode and Task-based Authentication mode. With Walk Up Authentication mode, all users must login before selecting a function to perform. In Task-based Authentication mode, a user first selects the task to be performed and then the TOE prompts for the user's authentication information. This allows Task-based Authentication mode to use different authentication mechanism for different tasks.

The two modes can and "must" be used simultaneously in the evaluated configuration. In the evaluated configuration, a user must first successfully authenticate using the Walk Up Authentication mode. If the Task-based Authentication mode uses a different authentication mechanism for the requested task, then the user will be required to successfully authenticate using the Task-based Authentication mode too.

When users authenticate through the Control Panel, the TOE displays asterisks for each character of a PIN or password typed to prevent onlookers from viewing another user's authentication data.

1.5.2.2.2 IPsec I&A

Networked computers can connect to the TOE to submit print jobs and to manage the TOE. The TOE uses IPsec to mutually authenticate computers that attempt to connect to them over the following interfaces:

- PJL
- HTTP (EWS)
- SNMP

IPsec is configured to use X.509v3 certificates via the Internet Key Exchange (IKE) protocol in the evaluated configuration.

The computers that attempt to connect with the TOE are classified as either Network Client Computers or Administrative Computers. The TOE uses IP addresses and the IPsec/Firewall to determine which computers are Network Client Computers and which are Administrative Computers.

Administrative Computers are allowed to connect to all interfaces listed above, whereas Network Client Computers are limited to just the PJL interface.

For day-to-day administration of the TOE, administrators use the HTTP interface (via EWS), the SNMP interface, and the PJL interface. Administrators typically use a web browser to interface with EWS. (Web browsers are part of the operational environment, not the TOE.) For SNMP, administrators typically use the HP Web Jetadmin application on an Administrative Computer to administer the TOE. (Web Jetadmin is part of the operational environment, not the TOE.) Web Jetadmin also communicates with the TOE using HTTP and PJL.

Because IPsec mutual authentication is performed at the computer level, not the user level, the computers allowed to access the TOE via EWS and SNMP must themselves be Administrative Computers. This means that non-TOE administrative users should not be allowed to log into the Administrative Computers because every user of an Administrative Computer is potentially a TOE administrator.

In addition, the TOE can contact many types of Authenticated Server Computers using IPsec and mutual authentication over the interfaces specified in section 1.5.4.1. The TOE contacts these computers either to send data to them (e.g. send a scanned object in an email to the SMTP Gateway) or to request information from them (e.g. authenticate a user using LDAP).These computers are known as Authenticated Server Computers because the TOE mutually authenticates theses servers prior to sending data to them. In these cases, the TOE acts like a client to these servers.

1.5.2.3 Data Protection and Access Control

1.5.2.3.1 Job PINs and Fax PINs

Users control access to print and copy jobs that they place in the TOE by assigning Job PINs to these jobs. Job PINs must be 4 digits in length. (The Job PIN length is enforced as an organizational policy.) This limits access to these jobs while they reside in the TOE and allows users to control when the jobs are printed so that physical access to the hardcopies can be controlled.

Administrators control the printing of analog faxes stored in Job Storage (i.e. Receive Fax in Table 1-1) by configuring an 8 digit Fax PIN in the TOE. The TOE then applies the Fax PIN to each Receive Fax job as the TOE receives the fax. This limits the access to the analog fax jobs stored in Job Storage to users who know the Fax PIN.

Some fax devices can hold a fax until another fax device requests that the fax be sent. Users can use the Fax Polling Receive function of the TOE to retrieve faxes from other fax devices. This is called a Fax Polling Receive job by this document. This feature does not require knowledge of the Fax PIN to receive and print a fax. To perform this function, the user authenticates to the TOE via the Control Panel and initiates the function by entering the phone number of the other fax device. The TOE will dial the other fax device and request the other fax device to transfer the held fax to the TOE via the currently active phone connection. The TOE prints the fax as it receives it. (The TOE does not accept polling requests from other fax devices (i.e. the TOE does not support the Fax Polling Send functionality).)

1.5.2.3.2 PJL Password

The TOE supports Printer Job Language (PJL) commands in print jobs. In the evaluated configuration, some PJL commands are password protected so that only authorized users can execute these PJL commands within their print jobs.

1.5.2.3.3 Residual Information Protection

The TOE protect deleted objects by making them unavailable via the TOE to TOE users. This prevents TOE users from attempting to recover deleted objects of other users through the TOE interfaces. In addition, the TOE provides Secure Storage Erase and Secure File Erase capabilities.

1.5.2.3.3.1 Secure Storage Erase

The TOE supports the overwriting of the hard drive in an HCD at the request of an administrator by using predefined algorithms. This helps prevent attackers from recovering data from these devices when these devices are used in other systems.

1.5.2.3.3.2 Secure File Erase

When documents are deleted from a hard drive, the TOE will overwrite the file in real-time. This helps prevent attackers from recovering data from these storage devices if these storage devices are removed from the HCD.

1.5.2.4 Protection of the TSF

1.5.2.4.1 Restricted Forwarding of Data

The TOE allows an administrator to restrict the forwarding of data received from an External Interface to the Shared-medium Interface. Specifically, the fax feature called “Archive to Email Address,” which can automatically archive received faxes to an email address, can be enabled / disabled by an administrator.

1.5.2.4.2 TSF Self-Testing

The TOE contains a suite of self-tests to test specific security functionality of the TOE. It contains data integrity checks for testing specific TSF data of the TOE and for testing the stored TOE executables.

1.5.2.4.3 Reliable Timestamps

The TOE contains a system clock that is used to generate reliable timestamps.

1.5.2.5 TOE Access Protection

1.5.2.5.1 Inactivity Timeout

The Control Panel supports an administrator selectable inactivity timeout in case users forget to logout of the Control Panel after logging in.

1.5.2.6 Trusted Channel Communication

The TOE supports the following mechanisms to protect data being transferred over the Shared-medium Interface:

- IPsec with X.509v3 certificates (for the Network Client Computer, Administrative Computer, SMTP gateway, HTTP (EWS), SNMP, PJL, LDAP, and remote file system interfaces)
- Kerberos (for the Kerberos interface)

In addition, the TOE provides certificate management for adding and deleting existing certificates.

1.5.2.7 Management

The TOE provides management capabilities for managing the TOE's functionality. The HCDs support the following user types: administrators, users, and authenticated servers. Administrators have the authority to manage the security functionality of the TOE and to manage users. Users can only manage user data that they have access to on the TOE. Authenticated servers are computers that are contacted by the TOE to perform services on behalf of the TOE.

1.5.3 TOE Boundaries

1.5.3.1 Physical

It is typical for an HCD to be shared by many users and for those users have direct physical access to the HCD. By design, users have easy access to some of the hardware features, such as the Control Panel (where users select to print, copy, etc.), the paper bins, the printer output trays, the scanner / copier, and the power switch. But other features such as the processor, firmware, and hard drive have more restricted access. These more restricted components are either more difficult to get to (such as the processor board) because they require hardware tools to disassemble the HCD or have a combination lock used to restrict access (such as to restrict access to the hard drive).

Note that because of the restricted access to the hard drive, the hard drive is considered as a non-removable nonvolatile storage device from the perspective of [2600.2].

Because of the physical accessibility of the HCDs, they must be used in non-hostile environments. Physical access should be controlled and/or monitored.

The TOE physical boundary is the HCD System Firmware (a.k.a. MFP Firmware) and Jetdirect Inside Firmware boundary and the English-language guidance documentation. The hardware is part of the operational environment.

1.5.3.2 Logical

The security functionality provide by the TOE has been described above. The following components are considered part of the operational environment and, therefore, beyond the scope of this evaluation:

- X.509v3 certificate generation
- HP Web Jetadmin administrative tool
- HP Printer Drivers for client computers (for submitting print job requests from Network Client Computers)
- Kerberos server
- LDAP server
- Remote file systems
- SMTP gateway
- syslog server
- Web browser
- HCD hardware

Regarding SMTP gateway, the TOE can only provide protection of sent emails to the device with which the TOE has the IPsec connection (i.e. the TOE only provides protection between the TOE and SMTP gateway). After that point, the operational environment must provide the remaining protection necessary to transfer the email from the SMTP gateway to the email's addressee(s).

1.5.3.3 Evaluated Configuration

The following items will need to be adhered to in the evaluated configuration:

- Only one Administrative Computer must be used to manage the TOE
- Third party applications cannot be installed on the TOE
- Control Panel Access Lock set to Maximum Menu Lock
- PC Fax Send disabled
- Fax Forwarding disabled
- Fax Archive to Fax Number for incoming faxes disabled

- Direct Ports disabled
- Remote Firmware Upgrade disabled
- Digital Sending Software (DSS) disabled
- Jetdirect Inside management via telnet & FTP disabled
- Jetdirect XML Services disabled
- File System External Access disabled
- IPsec authentication using X.509v3 certificates enabled (IPsec authentication using Kerberos or Pre-Shared Key is not supported)
- Walk Up and Task-based Authentication enabled
- SNMP support limited to:
    - SNMPv1 read-only
    - SNMPv2c read-only
    - SNMPv3

1.5.4 Security Policy Model

This section describes the security policy model for the TOE. Much of the terminology in this section comes from [2600.2] and is duplicated here so that readers won't have to read [2600.2] to understand the terminology used in the rest of this security target document.

1.5.4.1 Subjects/Users

Users are entities that are external to the TOE and which interact with the TOE. TOE users are defined in **Table 1-2**.

Table 1-2 - Users

Designation	Definition
U.USER	Any authorized User. Authorized Users are U.ADMINISTRATOR, U.NORMAL, and U.SERVER.
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE.
U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP).
U.SERVER	A User (trusted IT product entity) that the TOE authenticates and uses to provide additional services.

For the purpose of clarity in this security target, the following distinctions are made:

- **Control Panel users** – U.NORMAL users who physically access an HCD's Control Panel.
    - **Security attributes**: User Role
- **Incoming analog fax phone line users** – Unauthenticated entities that initiate and transmit faxes to the TOE over the HCD's analog fax phone line. These users are considered U.ADMINISTRATOR because User Document Data (i.e. incoming faxes) created by these users is considered to be owned by U.ADMINISTRATOR. There are no actual management / administrative functions available to these users.
    - **Security attributes:** None
- **Network Client Computers** – Computers (U.NORMAL entities) that can successfully authenticate to the TOE's PJL interface using IPsec and mutual authentication. The TOE will accept print jobs from any user of a computer where the computer has successfully authenticated to the TOE.
    - **Security attributes:** User Role and IP address
- **Administrative Computers** – Computers (U.ADMINISTRATOR entities) that can successfully authenticate to the TOE's administrative interfaces (i.e. HTTP/EWS and SNMP) using IPsec and mutual authentication. An Administrative Computer may also connect to the TOE as a Network Client Computer

(i.e. Administrative Computers can send print jobs as a U.NORMAL user through the PJL network interface).

- **Security attributes:** User Role and IP address

- **Server Computers** – Computers that provide services to the TOE. The TOE connects to Server Computers to request services from them. The Server Computers for the evaluated configuration are:
  - File system servers (i.e. CIFS servers and FTP servers)
  - Kerberos servers
  - LDAP servers
  - SMTP gateways
  - syslog servers

  Server Computers are a superset of Authenticated Server Computers.

- **Authenticated Server Computers** – Computers (U.SERVER entities) that are successfully authenticated by the TOE using IPsec and mutual authentication and that provide services to the TOE. The TOE connects to Authenticated Server Computers to request services from them. The Authenticated Server Computers for the evaluated configuration are:
  - File system servers (i.e. CIFS servers and FTP servers)
  - LDAP servers
  - SMTP gateways
  - syslog servers

  Authenticated Server Computers are a subset of Server Computers. As an example, the Kerberos server is a Server Computer, but is not an Authenticated Server Computer.
  - **Security attributes:** User Role and IP address

1.5.4.2 Objects

Objects are passive entities in the TOE that contain or receive information, and upon which Subjects perform Operations. Objects are equivalent to TOE Assets. There are three types of Objects:

- User Data
- TSF Data
- Functions

1.5.4.2.1 User Data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is comprised of two objects:

- User Document Data
- User Function Data

Table 1-3: User Data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user’s document. This includes the original document itself in hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user’s document or job to be processed by the TOE.

User data objects include:

- **Receive Fax jobs** – Fax jobs received by the TOE over the analog fax phone line where the connection is initiated by another fax device.
- **Fax Polling Receive jobs** – Fax jobs received by the TOE over the analog fax phone line where the connection is initiated by the TOE via the Fax Polling Receive function.
- **Send Fax jobs** – Fax jobs being sent by the TOE over the analog fax phone line. (The Send Fax functionality is available in the evaluated configuration, but the PC Fax Send feature is disabled in the evaluated configuration.)
- **Print job types that use Job Storage**:
    - **Personal print jobs** – Print jobs from a client computer that are stored in Job Storage. Optionally, they can be PIN protected with a Job PIN. These jobs are held until the user logs in to the Control Panel and releases the job. These print jobs can contain password protected PJL commands. These jobs are automatically deleted after printing or if the TOE is turned off or after an administrator specified time interval.
    - **Proof and hold print jobs** – Print jobs from a client computer where one proof copy is printed before printing additional copies. These jobs cannot be PIN protected. These jobs are automatically deleted after printing all requested copies or if the TOE is turned off or after an administrator specified time interval.
    - **Quick copy print jobs** – Print jobs from a client computer where all requested copies are printed and the job is left on (i.e. not deleted from) the TOE until the user deletes it or the TOE is turned off or after an administrator-specified time interval. These jobs cannot be PIN protected.
    - **Stored print jobs** – Print jobs such as a personnel form, time sheet, or calendar from a client computer that are stored indefinitely on the hardware controlled by theTOE and reprinted. Optionally, they can be PIN protected with a Job PIN. For PIN protected stored print jobs, the user (including the administrator) must know the Job PIN of the job in order to delete the job.
- **Send E-mail jobs** – Scan jobs that are scanned directly into an email and sent from the TOE to an SMTP gateway.
- **Send to Folder jobs** – Scan jobs that are saved to a remote file system.
- **Stored copy jobs** – A copy job that a Control Panel user has stored on the hardware controlled by the TOE. Stored copy jobs are scanned using the HCD's scanner, then stored by the TOE. Optionally, they can be PIN protected by the TOE with a Job PIN. For PIN protected stored copy jobs, the user (including the administrator) must know the Job PIN of the job in order to delete the job. Stored print jobs and stored copy jobs are similar except they originate from different methods.

1.5.4.2.2 TSF Data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is comprised of two components: TSF Protected Data and TSF Confidential Data.

Table 1-4 - TSF Data

Designation	Definition
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a user who is neither an administrator nor the owner of the data would have an effect on the operational security of the TOE.
D.PROT	TSF Protected Data are assets for which alteration by a user who is neither an administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

The following table lists the TSF Data and the data designations.

Table 1-5 - TSF Data Listing

TSF Data	D.CONF	D.PROT
Audit records and internal logs	X	

Cryptographic keys and certificates	X	
Device and network configuration settings		X
Job data including Job PINs	X	
Fax PIN	X	
PJL Password	X	
PJL protocol excluding the PJL Password, job data, and Job PINs		X
System time		X
User and Administrator identification data		X
User and Administrator authentication data	X	

1.5.4.3 SFR Package Functions

Functions perform processing, storage, and transmission of data. The following [2600.2]-defined functions apply to this security target.

Table 1-6 – SFR Package Functions

Designation	Definition
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

1.5.4.4 SFR Package Attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. The following [2600.2]-defined attributes apply to this security target.

Table 1-7 - SFR Package Attributes

Designation	Definition
+CPY	Indicates data that is associated with a copy job.
+DSR	Indicates data that is associated with a document storage and retrieval job.
+FAXIN	Indicates data that is associated with an inbound (received) fax job.
+FAXOUT	Indicates data that is associated with an outbound (sent) fax job.
+PRT	Indicates data that is associated with a print job.
+SCN	Indicates data that is associated with a scan job.
+SMI	Indicates data that is transmitted or received over a shared-medium interface.

2 Conformance Claims

2.1 Common Criteria

The ST is [CC] Part 2 extended and Part 3 conformant.

2.2 Packages

The ST claims an Evaluation Assurance Level of EAL2 augmented by ALC_FLR.2.

Common Criteria [CC] version 3.1 revision 2 is the basis for this conformance claim.

2.3 Protection Profiles

This Security Target claims demonstrable conformance to the following [2600.2] protection profile and packages since NIAP CCEVS Policy Letter #20 modifies IEEE Std 2600.2-2009:

- 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
- 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

Note: Although the HCDs in this Security Target contain a nonvolatile storage device (i.e. a hard drive), this nonvolatile storage device is considered an internal (built-in) component of the HCDs and, therefore, constitutes a non-removable nonvolatile storage device from the perspective of [2600.2]. Because no removable nonvolatile storage devices exist in the HCDs, this Security Target does **not** claim conformance to "2600.2-NVS SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B" contained in [2600.2].

The following table provides the mapping and rationale of how the SFRs in this Security Target map to the SFRs in [2600.2]. The term "n/a" means "not applicable".

Table 2-1 - SFR mappings between [2600.2] and the ST

[2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
Common SFRs				
FAU_GEN.1	FAU_GEN.1			The ST's FAU_GEN.1 combines the contents of FAU_GEN.1 from the common [2600.2] and FAU_GEN.1 from the [2600.2] SMI SFR package.
FAU_GEN.2	FAU_GEN.2			n/a
FDP_ACC.1(a)	FDP_ACC.1-cac			The ST's FDP_ACC.1-cac combines the contents of the FDP_ACC.1(a) from the common [2600.2] and the FDP_ACC.1's from the [2600.2] packages claimed by the ST. The iteration name was changed from "(a)" to "-cac" (Common Access Control) for better understandability when

				reading the ST.
FDP_ACC.1(b)	FDP_ACC.1-tfac			The iteration name was changed from “(b)” to “-tfac” (TOE Function Access Control) for better understandability when reading the ST.
FDP_ACF.1(a)	FDP_ACF.1-cac			The ST’s FDP_ACF.1-cac combines the contents of the FDP_ACF.1(a) from the common [2600.2] and the FDP_ACF.1’s from the [2600.2] packages claimed by the ST. The iteration name was changed from “(a)” to “-cac” (Common Access Control) for better understandability when reading the ST.
FDP_ACF.1(b)	FDP_ACF.1-tfac			The iteration name was changed from “(b)” to “-tfac” (TOE Function Access Control) for better understandability when reading the ST.
FDP_RIP.1	FDP_RIP.1			n/a
FIA_ATD.1	FIA_ATD.1			n/a
FIA_UAU.1	FIA_UAU.1, FIA_UAU.2-walkup, FIA_UAU.2-ipsec	X	X	The TOE’s Control Panel supports both Task-based (FIA_UAU.1) and Walkup (FIA_UAU.2-walkup) authentication which are both enabled simultaneously, and the TOE supports IPsec authentication (FIA_UAU.2-ipsec). The Walkup and IPsec comply with the more restrictive FIA_UAU.2.
FIA_UID.1	FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec	X	X	The TOE’s Control Panel supports both Task-based (FIA_UID.1) and Walkup (FIA_UID.2-walkup) identification which are both enabled simultaneously, and the TOE supports IPsec identification (FIA_UID.2-ipsec). The Walkup and IPsec comply with the more restrictive FIA_UID.2.
FIA_USB.1	FIA_USB.1			n/a
FMT_MSA.1(a)	FMT_MSA.1-cac, FMT_MSA.1-faxpin, FMT_MSA.1-pjl	X		FMT_MSA.1(a) was further iterated because either the operations on some of the security attributes differed or the authorised identified roles differed.
FMT_MSA.1(b)	FMT_MSA.1-tfac			The iteration name was changed from “(b)” to “-tfac” (TOE Function Access Control) for better understandability when

				reading the ST.
FMT_MSA.3(a)	FMT_MSA.3-cac, FMT_MSA.3-faxpin, FMT_MSA.3-pjl	X		FMT_MSA.3(a) was further iterated because either the operations on some of the security attributes differed or the authorised identified roles differed.
FMT_MSA.3(b)	FMT_MSA.3-tfac			The iteration name was changed from “(b)” to “-tfac” (TOE Function Access Control) for better understandability when reading the ST.
FMT_MTD.1.1(a)	FMT_MTD.1-certs, FMT_MTD.1-pins	X		The original reason for making these separate iterations is deprecated, but because all the evidence and reports were written using them both, they have been left as separate SFRs.
FMT_MTD.1.1(b)	FMT_MTD.1-users			The iteration name was changed from “(b)” to “-users” (TSF data associated with users) for better understandability when reading the ST.
FMT_SMF.1	FMT_SMF.1			n/a
FMT_SMR.1	FMT_SMR.1			n/a
FPT_STM.1	FPT_STM.1			n/a
FPT_TST.1	FPT_TST.1			n/a
FTA_SSL.3	FTA_SSL.3			n/a
CPY SFR Package				
FDP_ACC.1	FDP_ACC.1-cac	X		See rationale for FDP_ACC.1(a).
FDP_ACF.1	FDP_ACF.1-cac	X		See rationale for FDP_ACF.1(a).
DSR SFR Package				
FDP_ACC.1	FDP_ACC.1-cac	X		See rationale for FDP_ACC.1(a).
FDP_ACF.1	FDP_ACF.1-cac	X		See rationale for FDP_ACF.1(a).
FAX SFR Package				
FDP_ACC.1	FDP_ACC.1-cac	X		See rationale for FDP_ACC.1(a).
FDP_ACF.1	FDP_ACF.1-cac	X		See rationale for FDP_ACF.1(a).
PRT SFR Package				
FDP_ACC.1	FDP_ACC.1-cac	X		See rationale for FDP_ACC.1(a).
FDP_ACF.1	FDP_ACF.1-cac	X		See rationale for FDP_ACF.1(a).
SCN SFR Package				

FDP_ACC.1	FDP_ACC.1-cac	X		See rationale for FDP_ACC.1(a).
FDP_ACF.1	FDP_ACF.1-cac	X		See rationale for FDP_ACF.1(a).
SMI SFR Package				
FAU_GEN.1	FAU_GEN.1			The ST's FAU_GEN.1 combines the contents of FAU_GEN.1 from the common [2600.2] and FAU_GEN.1 from the [2600.2] SMI SFR package.
FPT_FDI_EXP.1	FPT_FDI_EXP.1			n/a
FTP_ITC.1	FTP_ITC.1			[CCEVS-PL20] adds User Data (D.DOC and D.FUNC) to the list of data in [2600.2] FTP_ITC.1.3.
Non-PP SFRs (SFRs in the ST, but not required by or hierarchical to SFRs in [2600.2])				
	FAU_STG.1			The TOE contains audit trail storage. Recommended by [2600.2] PP APPLICATION NOTE 5 and 7.
	FAU_STG.4			The TOE overwrites the oldest audit records in the audit trail. Recommended by [2600.2] PP APPLICATION NOTE 5 and 7.
	FDP_RIP_EXP.3			The TOE includes both a disk wiping feature and a file wiping feature which are separate security functionalities independent of the functionality that the TOE uses to support FDP_RIP.1.
	FIA_UAU.7			The TOE masks PINs and passwords. Recommended by [2600.2] PP APPLICATION NOTE 38.
	FMT_MOF.1-auth	X		The TOE allows administrators to select various authentication mechanisms; thus, changing the authentication behavior.
	FMT_MOF.1-ripstore	X		The TOE allows the administrator to change the behavior of the Secure Storage Erase feature.
	FMT_MOF.1-ripfile	X		The TOE allows the administrator to change the behavior of the Secure File Erase feature.

3 Security Problem Definition

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed.

To this end, the statement of TOE security environment identifies the list of assumptions made on the operational environment (including physical and procedural measures) and the intended method of use of the product, defines the threats that the product is designed to counter, and the organizational security policies with which the product is designed to comply.

3.2 Threats

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats

The threats and policies defined in this Security Target address the threats posed by these threat agents.

The threat agents are assumed to originate from a well managed user community in a non-hostile working environment. Therefore, the product protects against threats of security vulnerabilities that might be exploited in the intended environment for the TOE with medium level of expertise and effort. The TOE protects against straightforward or intentional breach of TOE security by attackers possessing a Basic attack potential.

3.2.1 Threats countered by the TOE

The threats identified in this section are addressed by the TOE.

Table 3-1 - Threats to User Data for the TOE

Threat	Affected asset	Description	From [2600.2]
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons	Yes
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons	Yes
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons	Yes

Table 3-2 - Threats to TSF Data for the TOE

Threat	Affected asset	Description	From [2600.2]
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons	Yes
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons	Yes
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons	Yes

3.3 Organizational Security Policies

The following Organizational Security Policies (OSPs) apply to the TOE:

Table 3-3 - Organizational security policies

Policy	Definition	From

		[2600.2]
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.	Yes
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.	Yes
P.PIN.LENGTHS	To protect access to documents and resources controlled by the TOE, users will create a 4 digit Job PIN for jobs that require Job PIN protection and the organization (e.g. administrators) will enforce an 8 digit Fax PIN, 8 digit User PINs, and a PJL Password of 9 or more digits.	No
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.	Yes
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.	Yes

3.4 Assumptions

This section indicates the minimum physical and procedural measures required to maintain security of the TOE.

3.4.1 Physical Aspects

Table 3-4 - Physical assumptions

Assumption	Definition	From [2600.2]
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.	Yes

3.4.2 Personnel Aspects

Table 3-5 - Personnel assumptions

Assumption	Definition	From [2600.2]
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.	Yes
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	Yes
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.	Yes

4 Security Objectives

4.1 Security Objectives for the TOE

All security objectives listed in this section are for the TOE.

Table 4-1 - Security objectives for the TOE

Objective	Definition	From [2600.2]
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration.	Yes
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.	Yes
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.	Yes
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.	Yes
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.	Yes
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.	Yes
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.	Yes
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.	Yes
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.	Yes
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.	Yes

4.2 Security Objectives for the Operational Environment

All security objectives listed in this section are for the operational environment.

Table 4-2 - Security Objectives for the Operational Environment

Objective	Definition	From [2600.2]
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer’s guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.	Yes
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.	Yes
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.	Yes
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order	Yes

	to detect potential security violations, and only by authorize persons.	
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.	Yes
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.	Yes
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.	Yes
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.	Yes
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.	Yes

4.3 Security Objective Rationale

The following tables provide a mapping of security objectives to the TOE and operational environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat, assumption or policy and that each threat, assumption or policy is covered by at least one security objective.

4.3.1 Security Objectives Coverage

Table 4-3- Completeness of security objectives

Objectives		**Threats, Policies, and Assumptions**													
	T.CONF.ALT	T.CONF.DIS	T.DOC.ALT	T.DOC.DIS	T.FUNC.ALT	T.PROT.ALT	P.AUDIT.LOGGING	P.INTERFACE.MANAGEMENT	P.PIN.LENGTHS	P.SOFTWARE.VERIFICATION	P.USER.AUTHORIZATION	A.ACCESS.MANAGED	A.ADMIN.TRAINING	A.ADMIN.TRUST	A.USER.TRAINING
O.AUDIT.LOGGED							X								
O.CONF.NO_ALT	X														
O.CONF.NO_DIS		X													
O.DOC.NO_ALT			X												
O.DOC.NO_DIS				X											
O.FUNC.NO_ALT					X										
O.INTERFACE.MANAGED								X							
O.PROT.NO_ALT						X									
O.SOFTWARE.VERIFIED										X					
O.USER.AUTHORIZED	X	X	X	X	X	X					X				

OE.ADMIN.TRAINED									X				X		
OE.ADMIN.TRUSTED														X	
OE.AUDIT.REVIEWED							X								
OE.AUDIT_ACCESS.AUTHORIZED							X								
OE.AUDIT_STORAGE.PROTECTED							X								
OE.INTERFACE.MANAGED								X							
OE.PHYSICAL.MANAGED												X			
OE.USER.AUTHORIZED	X	X	X	X	X	X					X				
OE.USER.TRAINED									X						X

4.3.2 Security Objectives Sufficiency

Table 4-4 - Security Objectives Sufficiency for Threats

Threats	Summary	Objectives and rationale
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons	O.CONF.NO_ALT protects D.CONF from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User Document Data may be altered by unauthorized persons	O.DOC.NO_ALT protects D.DOC from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons	O.PROT.NO_ALT protects D.PROT from unauthorized alteration. O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.

		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

Table 4-5 - Security Objectives Sufficiency for Policies

Policies	Summary	Objectives and rationale
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration. OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modifications. OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records. OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies. OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
P.PIN.LENGTHS	Minimum required lengths for Job PINs, the Fax PIN, User PINs, and the PJL Password.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training including the proper lengths of PIN and password values. OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training including the proper lengths of Job PIN values.
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.USER.AUTHORIZATION	Users will be authorized to use the TOE.	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE. OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.

Table 4-6 - Security Objectives Sufficiency for Assumptions

Assumptions	Summary	Objectives and rationale
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.

	data interfaces of the TOE.	
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5 Extended Components Definition

5.1 FDP_RIP_EXP.3

The Security Target defines the extended component FDP_RIP_EXP.3 as part of the FDP_RIP family in CC Part 2 for use within this ST.

5.1.1 Component leveling

FDP_RIP_EXP.3 is not hierarchical to any other component within the FDP_RIP family.

FDP_RIP_EXP.3 Nonvolatile storage residual information protection requires that the TSF provide one or more methods to overwrite data on nonvolatile storage.

5.1.2 Management: FDP_RIP_EXP.3

The following action could be considered for the management functions in FMT:

a) The choice of when to overwrite the nonvolatile storage could be made configurable within the TOE.

b) The choice of overwrite algorithms could be made configurable within the TOE.

5.1.3 Audit: FDP_RIP_EXP.3

There are no auditable events foreseen.

5.1.4 FDP_RIP_EXP.3 Nonvolatile Storage Residual Information Protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP_EXP.3.1 The TSF shall overwrite all accessible blocks of the hard drive using pre-defined algorithms at the request of U.ADMINISTRATOR.

FDP_RIP_EXP.3.2 The TSF shall overwrite User Document Data during deletion using pre-defined algorithms selected by U.ADMINISTRATOR.

5.1.5 Rationale

Although [2600.2] includes FDP_RIP.1 for residual information protection under normal TOE usage, FDP_RIP.1 does not protect against the internal hard drive being removed from the HCD (e.g. by theft, by service personnel) or for the case where the HCD is being repurposed (e.g. the HCD was leased, the lease has expired, and now the HCD is being removed from its protected environment and returned to the lessor).

Element FDP_RIP_EXP.3.1 addresses the issue of the HCD being repurposed. By overwriting the sectors of a hard drive, the information on the hard drive, including formatting information, is made inaccessible from normal means of reading information from a hard drive including the reading of the drive as a "raw" device.

Element FDP_RIP_EXP.3.2 addresses the issue of residual User Document Data remaining on the hard drive when the document is logically deleted by the user. By overwriting the User Document Data, the data is made inaccessible from normal means of reading information from a hard drive including the reading of the drive as a "raw" device.

6 Security Requirements

6.1 TOE Security Functional Requirements

SFR refinements are marked in **bold**. SFR assignments are marked in [**bold**]. SFR selections are marked in [***italic bold***]. SFR text deletions are marked with ~~strikethroughs~~.

6.1.1 Security Audit (FAU)

6.1.1.1 Audit Data Generation (FAU_GEN.1)

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

- Start-up and shutdown of the audit functions; **and**
- All auditable events for the [***not specified***] level of audit; and
- [**All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in ~~Table 15~~ Table 6-1; [none]**]~~.~~

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**for each Relevant SFR listed in ~~Table 15~~ Table 6-1: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [**none**]]~~.~~

Table 6-1 - Auditable Events

Auditable event	Relevant SFR(s)	Audit level	Additional information	[2600.2]
Job completion	FDP_ACF.1-tfac	Not specified	Type of job	No
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1, FIA_UAU.2-ipsec, FIA_UAU.2-walkup	Basic	None required	Yes: Common
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1, FIA_UID.2-ipsec, FIA_UID.2-walkup	Basic	Attempted user identity, if available	Yes: Common
Use of the management functions	FMT_SMF.1	Minimum	None required	Yes: Common
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required	Yes: Common
Changes to the time	FPT_STM.1	Minimum	None required	Yes: Common
Locking of an interactive session by the session locking mechanism	FTA_SSL.3	Minimum	None required	No
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required	Yes: SMI

6.1.1.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 Protected Audit Trail Storage (FAU_STG.1)

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

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

6.1.1.4 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [**none**] if the audit trail is full.

6.1.2 User Data Protection (FDP)

6.1.2.1 Common Access Control SFP (FDP_ACC.1-cac)

FDP_ACC.1.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2**] on [**the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in ~~Table 17~~ Table 6-2**].

Table 6-2 - Common Access Control SFP

Object	Operation(s)	Subject	Access control rules	[2600.2] Section
D.FUNC	Modify; Delete	U.NORMAL	For scan and print objects in Job Storage with the Job PIN attribute set: Subjects must know the Job PIN to delete and/or modify the object; otherwise, delete and modify access is denied. For print objects: Subjects must know the PJL Password in order to execute password protected PJL commands that modify and delete D.FUNC; otherwise, password protected PJL command requests are denied. For Receive Fax objects: Subjects must know the Fax PIN to delete the objects; otherwise, delete access is denied. Modify access is denied to all subjects. For Fax Polling Receive objects: The subject performing the polling fax function can delete	Common

			the received object (i.e. the TOE automatically deletes the object at the end of the function); otherwise, delete access is denied. Modify access is denied to all subjects. Send Fax objects cannot be deleted or modified.	
D.DOC	Delete	U.NORMAL	For scan and print objects in Job Storage with the Job PIN attribute set: Subjects must know the Job PIN to delete the object; otherwise, delete access is denied. For print objects: Subjects must know the PJL Password in order to execute password protected PJL commands that delete D.DOC; otherwise, password protected PJL command requests are denied. For Receive Fax objects: Subjects must know the Fax PIN to delete the objects; otherwise, delete access is denied. For Fax Polling Receive objects: The subject performing the outbound fax polling function can delete the object (i.e. the TOE automatically deletes the object at the end of the function); otherwise, delete access is denied. Send Fax objects cannot be deleted.	Common
D.DOC+DSR D.DOC+PRT D.DOC+SCN	Read	U.NORMAL	For scan and print objects in Job Storage with the Job PIN attribute set: Subjects must know the Job PIN to read the object; otherwise, read access is denied.	DSR, PRT, SCN
D.DOC+FAXIN D.DOC+FAXOUT	Read	U.NORMAL	(D.DOC+FAXIN) For Receive Fax objects: Subjects must be authorized by U.ADMINISTRATOR (i.e. know the Fax PIN) to read the objects;	FAX

			otherwise, read access is denied. For Fax Polling Receive objects: The subject performing the outbound fax polling function can read the object; otherwise, read access is denied. (D.DOC+FAXOUT) Send Fax objects cannot be read by any subject.	
D.DOC+CPY	Read; Modify	U.NORMAL	There are no access control restrictions for read and modify access.	CPY

6.1.2.2 TOE Function Access Control SFP (FDP_ACC.1-tfac)

FDP_ACC.1.1 The TSF shall enforce the [**TOE Function Access Control SFP**] on [**users as subjects, TOE functions as objects, and the right to use the functions as operations**].

6.1.2.3 Common Access Control Functions (FDP_ACF.1-cac)

FDP_ACF.1.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2]** to objects based on the following: [**the list of users as subjects and objects controlled under the Common Access Control SFP in ~~Table 17~~ Table 6-2, and for each, the indicated security attributes in ~~Table 17~~ Table 6-2**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**rules specified in the Common Access Control SFP in ~~Table 17~~ Table 6-2 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

- **For scan and print objects: If the Job PIN attribute is not set, all U.NORMAL subjects can read and delete D.DOC for these objects and can modify and delete D.FUNC for these objects**
- **U.ADMINISTRATOR can delete any D.DOC (including D.FUNC) except for stored print jobs with Job PINs and stored copy jobs with Job PINs**
- **U.ADMINISTRATOR can modify D.FUNC**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**following additional rules: none**].

6.1.2.4 TOE Function Access Control Functions (FDP_ACF.1-tfac)

FDP_ACF.1.1 The TSF shall enforce the [**TOE Function Access Control SFP**] to objects based on the following: [**users and [the following TOE functions and security attributes:**

- **Users: {Control Panel users}; Functions: {F.CPY, F.DSR, F.FAX, F.PRT, F.SCN, F.SMI}; Security attributes: {User Role}**
- **Users: {Network Client Computers}; Functions: {F.DSR, F.PRT, F.SMI}; Security attributes: {User Role, X.509v3 certificate, IP address}**
- **Users: {Administrative Computers}; Functions: {F.SMI}; Security attributes: {User Role, X.509v3 certificate, IP address}**]].

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

- ***the user is explicitly authorized by U.ADMINISTATOR to use a function***

- ***a* Network Client Computer ~~*user*~~ *that is authorized to use the TOE is automatically authorized to use the functions* [F.DSR, F.PRT, F.SMI]]]**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the user acts in the role U.ADMINISTRATOR: [none]**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**following additional rules: none**].

6.1.2.5 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [**D.DOC, [none]**].

6.1.2.6 Nonvolatile Storage Residual Information Protection (FDP_RIP_EXP.3)

FDP_RIP_EXP.3.1 The TSF shall overwrite all accessible blocks of the hard drive using pre-defined algorithms at the request of U.ADMINISTRATOR.

FDP_RIP_EXP.3.2 The TSF shall overwrite User Document Data during deletion using pre-defined algorithms selected by U.ADMINISTRATOR.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 Local User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **User Role (defined in FMT_SMR.1)**
- **Control Panel user's User PIN for User PIN Authentication**
- **IP address of Network Client Computers and Administrative Computers].**

6.1.3.2 Timing of Task-based Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**the following Control Panel TSF-mediated actions**] on behalf of the **Control Panel** user to be performed before the user is authenticated **when the Task-based Authentication mode is configured to use a different authentication mechanism than the Walk Up Authentication mechanism uses:**

- **Walk Up Authentication**
- **Selection of the Copy operation**
- **Selection of the Color Copy (Color LaserJets only) operation**
- **Selection of the Send E-mail operation**
- **Selection of the Send Fax operation**
- **Selection of the Send to Folder operation**
- **Selection of the Job Storage (includes printing of stored jobs and incoming faxes) operation**
- **Selection of the Create Stored Copy Job operation**
- **Selection of the Administration operation**
- **Selection of the Simplex Copy (one-sided copy) operation**.

FIA_UAU.1.2 The TSF shall require each **Control Panel** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: In the evaluated configuration, the Administration operation only allows a user to print the Blocked Fax list and the Speed Dial list.

6.1.3.3 Walk Up User Authentication before Any Action (FIA_UAU.2-walkup)

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

6.1.3.4 IPsec Authentication before Any Action (FIA_UAU.2-ipsec)

FIA_UAU.2.1 The TSF shall require each **Network Client Computer, Administrative Computer, and Authenticated Server Computer connection** ~~user~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **connection** ~~user~~.

6.1.3.5 Control Panel Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only [**asterisk characters for each PIN digit typed and for each password character typed**] to the user while the **Control Panel** authentication is in progress.

6.1.3.6 Timing of Task-based Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**the following Control Panel TSF-mediated actions**] on behalf of the **Control Panel** user to be performed before the user is identified **when the Task-based Authentication mode is configured to use a different authentication mechanism than the Walk Up Authentication mechanism uses:**

- **Walk Up Authentication**
- **Selection of the Copy operation**
- **Selection of the Color Copy (Color LaserJets only) operation**
- **Selection of the Send E-mail operation**
- **Selection of the Send Fax operation**
- **Selection of the Send to Folder operation**
- **Selection of the Job Storage (includes printing of stored jobs and incoming faxes) operation**
- **Selection of the Create Stored Copy Job operation**
- **Selection of the Administration operation**
- **Selection of the Simplex Copy (one-sided copy) operation**.

FIA_UID.1.2 The TSF shall require each **Control Panel** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: In the evaluated configuration, the Administration operation only allows a user to print the Blocked Fax list and the Speed Dial list.

6.1.3.7 Walk Up User Identification before Any Action (FIA_UID.2-walkup)

FIA_UID.2.1 The TSF shall require each **Control Panel** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.8 Network Client Computer Identification before Any Action (FIA_UID.2-ipsec)

FIA_UID.2.1 The TSF shall require each **Network Client Computer, Administrative Computer, and Authenticated Server Computer connection** ~~user~~ to be successfully identified before allowing any other TSF-mediated actions on behalf of that **connection** ~~user~~.

6.1.3.9 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**User Role**].

Application Note: Incoming analog fax phone line users have no security attributes, but Receive Fax jobs are owned by U.ADMINISTRATOR.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on the behalf of users: [**none**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with the subjects acting on the behalf of users: [**none**].

6.1.4 Security Management (FMT)

6.1.4.1 Management of Authentication Security Functions Behavior (FMT_MOF.1-auth)

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable, modify the behavior of***] the function~~s~~ [**authentication**] to [**U.ADMINISTRATOR**].

6.1.4.2 Management of Secure Storage Erase Security Functions Behavior (FMT_MOF.1-ripstore)

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable, modify the behavior of***] the function~~s~~ [**Secure Storage Erase**] to [**U.ADMINISTRATOR**].

6.1.4.3 Management of Secure File Erase Security Functions Behavior (FMT_MOF.1-ripfile)

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable, modify the behavior of***] the function~~s~~ [**Secure File Erase**] to [**U.ADMINISTRATOR**].

6.1.4.4 Management of Common Security Attributes (FMT_MSA.1-cac)

FMT_MSA.1.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to restrict the ability to [***set***] the security attribute~~s~~ [**Job PIN**] to [**the subject creating the Job PIN-protected objects defined in FDP_ACC.1-cac**].

6.1.4.5 Management of Fax PIN Security Attribute (FMT_MSA.1-faxpin)

FMT_MSA.1.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to restrict the ability to [***set, modify***] the security attribute~~s~~ [**Fax PIN**] to [**U.ADMINISTRATOR**].

Application Note: The product allows authorized administrators to delete the Fax PIN, but they should not delete the Fax PIN in the evaluated configuration.

6.1.4.6 Management of PJL Password-based Security Attributes (FMT_MSA.1-pjl)

FMT_MSA.1.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to restrict the ability to [***set, modify***] the security attribute~~s~~ [**PJL Password**] to [**anyone (i.e. U.ADMINISTRATOR and/or U.NORMAL) who knows the PJL Password**].

Application Note: The product allows for the deletion of the PJL Password, but the PJL Password should not be deleted in the evaluated configuration.

6.1.4.7 Management of TOE Function Security Attributes (FMT_MSA.1-tfac)

FMT_MSA.1.1 The TSF shall enforce the [**TOE Function Access Control SFP, [none]**] to restrict the ability to [***set, modify***] the security attribute~~s~~ [**User Role, X509v3 certificate, IP address**] to [**U.ADMINISTRATOR**].

6.1.4.8 Common Static Attribute Initialization (FMT_MSA.3-cac)

FMT_MSA.3.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to provide [***permissive***] default values for security attributes **defined in FMT_MSA.1-cac** that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**subject creating a Job PIN-protected object defined in FDP_ACC.1-cac**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.9 Fax PIN Static Attribute Initialization (FMT_MSA.3-faxpin)

FMT_MSA.3.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to provide [***restrictive***] default values for security attributes **defined in FMT_MSA.1-faxpin** that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**U.ADMINISTRATOR**] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The Fax PIN assigned to a Receive Fax job is the value of the current Fax PIN.

6.1.4.10 PJL Password-based Static Attribute Initialization (FMT_MSA.3-pjl)

FMT_MSA.3.1 The TSF shall enforce the [**Common Access Control SFP in ~~Table 17~~ Table 6-2, [none]**] to provide [***restrictive***] default values for security attributes **defined in FMT_MSA.1-pjl** that are used to enforce the SFP.

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

Application Note: Because certain PJL commands are the objects of the PJL Password security attribute and PJL commands cannot be created, an alternative initial value cannot be specified; thus, “Nobody” is used to indicate that an alternative initial value cannot be specified.

6.1.4.11 TOE Function Static Attribute Initialization (FMT_MSA.3-tfac)

FMT_MSA.3.1 The TSF shall enforce the [**TOE Function Access Control Policy, [none]**] to provide [***restrictive***] default values for security attributes **defined in FMT_MSA.1-tfac** that are used to enforce the SFP.

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

6.1.4.12 Management of TSF Data (FMT_MTD.1-certs)

FMT_MTD.1.1 The TSF shall restrict the ability to [***perform operations specified below for***] the [

- **Jetdirect certificate: overwrite operation**
- **Certificate Authority (CA) certificate: add, delete operations**]

to [***U.ADMINISTRATOR***].

6.1.4.13 Management of TSF Data (FMT_MTD.1-pins)

FMT_MTD.1.1 The TSF shall restrict the ability to [***initialize, modify***] the [

- **Fax PIN**
- **Allowed IP addresses for Network Client Computers, Administrative Computers, and Server Computers**]

to [***U.ADMINISTRATOR***].

6.1.4.14 Management of TSF Data (FMT_MTD.1-users)

FMT_MTD.1.1 The TSF shall restrict the ability to [***initialize, modify***] the [**User PINs**] to [***U.ADMINISTRATOR***].

6.1.4.15 Specification of Management Functions (FMT_SMF.1)

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

- **Authentication selection management**

- **User PIN Authentication data management**
- **Fax PIN management**
- **PJL Password management**
- **Secure Storage Erase management**
- **Secure File Erase management**
- **X.509v3 Certificate management**
- **IP address management for Network Client Computers, Administrative Computers, and Server Computers**].

6.1.4.16 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**U.ADMINISTRATOR, U.NORMAL, [*Nobody, U.SERVER*]**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated**.

Application Note: There is no actual role called "Nobody" in the HCD. "Nobody" is an artificial role created by [2600.2] to aid in explanation of concepts in [2600.2].

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Restricted Forwarding of Data to External Interfaces (FPT_FDI_EXP.1)

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [**any external Interface**] from being forwarded without further processing by the TSF to [**any Shared-medium Interface**].

6.1.5.2 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.5.3 TSF Testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests [***at the request of the authorised user***] to demonstrate the correct operation of [

- ***PJL Password***
- ***System Clock***
- ***User PIN Authentication (if configured)***
- ***LDAP Authentication (if configured)***
- ***Kerberos Authentication (if configured)***].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [

- ***PJL Password***
- ***User PIN authentication database***
- ***Bootloader password***
- ***Fax PIN***
- ***Control Panel authentication configuration data for the Copy, Color Copy, Send E-mail, Send Fax, Send to Folder, Job Storage, Create Stored Copy Job, Administration, and Simplex Copy operations***].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.6 TOE Access (FTA)

6.1.6.1 Control Panel TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate ~~an~~ **a Control Panel** interactive session after a [**U.ADMINISTRATOR configurable time interval of user inactivity**].

6.1.7 Inter-TSF Trusted Channel (FTP)

6.1.7.1 Inter-TSF Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the **communicated** ~~channel~~ data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF, another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**].

6.2 Security Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of the SFRs to the security objectives showing that each security functional requirement addresses at least one objective and that each objective maps to at least one SFR. The [2600.2] SFRs and objects and the additional SFRs and objectives not covered by [2600.2] are separated in the table by a grey line.

Table 6-3 - Completeness of security requirements

	Objective									
SFR	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED
FAU_GEN.1										X
FAU_GEN.2										X
FDP_ACC.1-cac	X	X	X							
FDP_ACC.1-tfac							X			
FDP_ACF.1-cac	X	X	X							
FDP_ACF.1-tfac							X			
FDP_RIP.1	X									
FIA_ATD.1							X			
FIA_UAU.1							X	X		
FIA_UAU.2-walkup							X	X		
FIA_UAU.2-ipsec							X	X		
FIA_UID.1	X	X	X	X	X	X	X	X		X

FIA_UID.2-walkup	X	X	X	X	X	X	X	X		X
FIA_UID.2-ipsec	X	X	X	X	X	X	X	X		X
FIA_USB.1							X			
FMT_MSA.1-cac	X	X	X							
FMT_MSA.1-faxpin	X	X	X							
FMT_MSA.1-pjl	X	X	X							
FMT_MSA.1-tfac							X			
FMT_MSA.3-cac	X	X	X							
FMT_MSA.3-faxpin	X	X	X							
FMT_MSA.3-pjl	X	X	X							
FMT_MSA.3-tfac							X			
FMT_MTD.1-certs				X	X	X				
FMT_MTD.1-pins				X	X	X				
FMT_MTD.1-users				X	X	X				
FMT_SMF.1	X	X	X	X	X	X				
FMT_SMR.1	X	X	X	X	X	X	X			
FPT_FDI_EXP.1								X		
FPT_STM.1										X
FPT_TST.1									X	
FTA_SSL.3							X	X		
FTP_ITC.1	X	X	X	X	X	X				
FAU_STG.1										X
FAU_STG.4										X
FDP_RIP_EXP.3	X				X					
FIA_UAU.7					X					
FMT_MOF.1-auth				X						
FMT_MOF.1-ripstore		X	X	X		X				
FMT_MOF.1-ripfile				X						

6.2.2 Sufficiency

[2600.2] contains the sufficiency arguments for the [2600.2] SFRs and objectives. The following table contains the security requirements sufficiency rationale for the SFRs and objectives not covered by [2600.2].

Table 6-4 - Additional security requirements sufficiency rationale

Security Objective	Rationale
O.AUDIT.LOGGED	The objective that: • the TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration is met by: • [FAU_GEN.1] which enforces audit policies by requiring logging of relevant events • [FAU_GEN.2] which enforces audit policies by requiring logging of information associated with audited events • [FAU_STG.1] which protects the audit trail from unauthorized deletion and prevents unauthorized modifications to the records in the audit log • [FAU_STG.4] which specifies how the audit log maintains audit records when the log is full • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support audit policies by associating user identity with events • [FPT_STM.1] which supports audit policies by requiring time stamps associated with events
O.CONF.NO_ALT	The objective that:

	• the TOE shall protect TSF Confidential Data from unauthorized alteration is met by: • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MOF.1-ripstore] which specifies the roles that can manage and the management controls available for the overwriting of internal hard drives • [FMT_MTD.1-certs, FMT_MTD.1-pins, FMT_MTD.1-users] which enforce protection by restricting access • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.CONF.NO_DIS	The objective that: • the TOE shall protect TSF Confidential Data from unauthorized disclosure is met by: • [FDP_RIP_EXP.3] which specifies that all accessible blocks of a hard drive are overwritten using pre-defined algorithms at the request of an administrator • [FIA_UAU.7] which masks the display of certain passwords and PINs during authentication • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MTD.1-certs, FMT_MTD.1-pins, FMT_MTD.1-users] which enforce protection by restricting access • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.DOC.NO_ALT	The objective that: • the TOE shall protect User Document Data from unauthorized alteration is met by: • [FDP_ACC.1-cac] which enforces protection by establishing an access control policy • [FDP_ACF.1-cac] which supports access control policy by providing access control function • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MOF.1-ripstore] which specifies the roles that can manage and the management controls available for the overwriting of internal hard drives • [FMT_MSA.1-cac, FMT_MSA.1-faxpin, FMT_MSA.1-pjl] which

	support access control function by enforcing control of security attributes • [FMT_MSA.3-cac, FMT_MSA.3-faxpin, FMT_MSA.3-pjl] which support access control function by enforcing control of security attribute defaults • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.DOC.NO_DIS	The objective that: • the TOE shall protect User Document Data from unauthorized disclosure is met by: • [FDP_ACC.1-cac] which enforces protection by establishing an access control policy • [FDP_ACF.1-cac] which supports access control policy by providing access control function • [FDP_RIP.1] which enforces protection by making residual data unavailable • [FDP_RIP_EXP.3] which specifies that User Document Data are overwritten using pre-defined algorithms when deleted • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MSA.1-cac, FMT_MSA.1-faxpin, FMT_MSA.1-pjl] which support access control function by enforcing control of security attributes • [FMT_MSA.3-cac, FMT_MSA.3-faxpin, FMT_MSA.3-pjl] which support access control function by enforcing control of security attribute defaults • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.FUNC.NO_ALT	The objective that: • the TOE shall protect User Function Data from unauthorized alteration is met by: • [FDP_ACC.1-cac] which enforces protection by establishing an access control policy • [FDP_ACF.1-cac] which supports access control policy by providing access control function • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MOF.1-ripstore] which specifies the roles that can manage and the management controls available for the overwriting of internal hard

	drives • [FMT_MSA.1-cac, FMT_MSA.1-faxpin, FMT_MSA.1-pjl] which support access control function by enforcing control of security attributes • [FMT_MSA.3-cac, FMT_MSA.3-faxpin, FMT_MSA.3-pjl] which support access control function by enforcing control of security attribute defaults • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.INTERFACE.MANAGED	The objective that: • the TOE shall manage the operation of external interfaces in accordance with security policies is met by: • [FIA_UAU.1, FIA_UAU.2-walkup, FIA_UAU.2-ipsec] which enforce management of external interfaces by requiring user authentication • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which enforce management of external interfaces by requiring user identification • [FPT_FDI_EXP.1] which enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces • [FTA_SSL.3] which enforces management of external interfaces by terminating inactive sessions
O.PROT.NO_ALT	The objective that: • the TOE shall protect TSF Protected Data from unauthorized alteration is met by: • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which support access control and security roles by requiring user identification • [FMT_MOF.1-auth] which specifies the roles that can manage and the management controls available for the authentication function • [FMT_MOF.1-ripstore] which specifies the roles that can manage and the management controls available for the overwriting of internal hard drives • [FMT_MOF.1-ripfile] which specifies the roles that can manage and the management controls available for the overwriting of deleted User Document Data • [FMT_MTD.1-certs, FMT_MTD.1-pins, FMT_MTD.1-users] which enforce protection by restricting access • [FMT_SMF.1] which supports control of security attributes by requiring functions to control attributes • [FMT_SMR.1] which supports control of security attributes by requiring security roles • [FTP_ITC.1] which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.SOFTWARE.VERIFIED	The objective:

	• the TOE shall provide procedures to self-verify executable code in the TSF is met by: • [FPT_TST.1] which enforces verification of software by requiring self-tests
O.USER.AUTHORIZED	The objective that: • the TOE shall require identification and authentication of Users, and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE is met by: • [FDP_ACC.1-tfac] which enforces authorization by establishing an access control policy • [FDP_ACF.1-tfac] which supports access control policy by providing access control function • [FIA_ATD.1] which supports authorization by associating security attributes with users • [FIA_UAU.1, FIA_UAU.2-walkup, FIA_UAU.2-ipsec] which enforce authorization by requiring user authentication • [FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec] which enforce authorization by requiring user identification • [FIA_USB.1] which enforces authorization by distinguishing subject security attributes associated with user roles • [FMT_MSA.1-tfac] which support access control function by enforcing control of security attributes • [FMT_MSA.3-tfac] which support access control function by enforcing control of security attribute defaults • [FMT_SMR.1] which supports authorization by requiring security roles • [FTA_SSL.3] which enforces authorization by terminating inactive sessions

6.2.3 Security Requirements Dependency Analysis

The following table shows the dependencies between the different security functional requirements and if they are resolved in this Security Target.

Table 6-5 - Dependencies between SFRs

SFR	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1; FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FDP_ACC.1-cac	FDP_ACF.1 Security attribute based access control	FDP_ACF.1-cac
FDP_ACC.1-tfac	FDP_ACF.1 Security attribute based access control	FDP_ACF.1-tfac
FDP_ACF.1-cac	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1-cac; FMT_MSA.3-cac, FMT_MSA.3-faxpin, FMT_MSA.3-pjl
FDP_ACF.1-tfac	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1-tfac; FMT_MSA.3-tfac
FDP_RIP.1	No dependencies	
FDP_RIP_EXP.3	No dependencies	
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.2-walkup	FIA_UID.1 Timing of identification	FIA_UID.2-walkup
FIA_UAU.2-ipsec	FIA_UID.1 Timing of identification	FIA_UID.2-ipsec
FIA_UAU.7	FIA_UAU.1 Timing of authentication	FIA_UAU.1, FIA_UAU.2-walkup
FIA_UID.1	No dependencies	
FIA_UID.2-walkup	No dependencies	
FIA_UID.2-ipsec	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1-auth	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FMT_MOF.1-ripstore	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FMT_MOF.1-ripfile	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1

FMT_MSA.1-cac	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
		FDP_ACC.1-cac;
		FMT_SMF.1;
		FMT_SMR.1

FMT_MSA.1-faxpin	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
		FDP_ACC.1-cac;
		FMT_SMF.1;
		FMT_SMR.1

FMT_MSA.1-pjl	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
		FDP_ACC.1-cac;
		FMT_SMF.1;
		FMT_SMR.1

FMT_MSA.1-tfac	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
		FDP_ACC.1-tfac;
		FMT_SMF.1;
		FMT_SMR.1

FMT_MSA.3-cac	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1-cac; FMT_SMR.1
FMT_MSA.3-faxpin	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1-faxpin; FMT_SMR.1
FMT_MSA.3-pjl	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1-pjl; FMT_SMR.1
FMT_MSA.3-tfac	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1-tfac; FMT_SMR.1
FMT_MTD.1-certs	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FMT_MTD.1-pins	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FMT_MTD.1-users	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1, FIA_UID.2-walkup, FIA_UID.2-ipsec
FPT_FDI_EXP.1	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	FMT_SMF.1; FMT_SMR.1
FPT_STM.1	No dependencies	
FPT_TST.1	No dependencies	
FTA_SSL.3	No dependencies	
FTP_ITC.1	No dependencies	

6.3 Security Assurance Requirements

The target evaluation assurance level for the TOE is EAL2 [CC] augmented by ALC_FLR.2 as specified in [CC] Part 3. No operations are applied to the assurance components.

Table 6-6: Security assurance requirements

Security assurance class	Security assurance requirement	Source
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3
	ADV_TDS.1 Basic design	CC Part 3
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3
	AGD_PRE.1 Preparative procedures	CC Part 3
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3
	ALC_DEL.1 Delivery procedures	CC Part 3
	ALC_FLR.2 Flaw reporting procedures	CC Part 3
ASE Security Target evaluation	ASE_CCL.1 Conformance claims	CC Part 3
	ASE_ECD.1 Extended components definition	CC Part 3
	ASE_INT.1 ST introduction	CC Part 3
	ASE_OBJ.2 Security objectives	CC Part 3
	ASE_REQ.2 Derived security requirements	CC Part 3
	ASE_SPD.1 Security problem definition	CC Part 3
	ASE_TSS.1 TOE summary specification	CC Part 3
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3
	ATE_FUN.1 Functional testing	CC Part 3
	ATE_IND.2 Independent testing - sample	CC Part 3
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match a Basic attack potential commensurate with the threat environment that is experienced by typical consumers of the TOE and commensurate with [2600.2]. In addition, the evaluation assurance level has been augmented with ALC_FLR.2 commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level and commensurate with [2600.2].

7 TOE Summary Specification

The following section explains how the security functions are implemented by the TOE. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Auditing
- Identification and Authentication
- Data Protection and Access Control
- Protection of the TSF
- TOE Access Protection
- Trusted Channel Communication
- Management

7.1 Auditing

The TOE performs auditing of security relevant functions. The TOE maintains an internal, fixed-size audit log file for storage of audited events and protects the log from non-administrative (U.NORMAL) access, including unauthorized deletion and modification of records. The TOE overwrites the oldest stored audit records in the log file when the log is full.

The TOE also connects and sends records to a syslog server (part of the operational environment) for long-term storage and audit review. The events sent to the syslog server by the TOE are only those generated by the TOE while the syslog server has an established connection. If the connection between the TOE and syslog server breaks but is later reestablished, only events generated by the TOE after the connection is reestablished are sent to the syslog server.

The types of records generated by the TOE are specified in section 6.1.1.1. Each record includes the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Events resulting from actions of identified users are associated with the identity of the user that caused the event. The timestamps on the audit records are generated from the TOE's clock function.

This section maps to the following SFRs:

- FAU_GEN.1
- FAU_GEN.2
- FAU_STG.1
- FAU_STG.4
- FPT_STM.1

7.2 Identification and Authentication (I&A)

The TOE supports multiple authentication mechanisms, both local and remote. This section describes the supported mechanisms.

The following interfaces support I&A:

- Control Panel
- IPsec (Network Client Computer & Administrative Computers)

The following interface allows a user limited TOE access without I&A:

- Analog Fax Phone Line (for incoming analog fax phone line users)

7.2.1 Control Panel I&A

The Control Panel interface supports both local and remote authentication mechanisms and allows only non-administrative users (i.e. U.NORMAL) to log in through this interface. The interface supports two modes of authentication:

- Task-based Authentication mode (a.k.a. “Device Functions”)
- Walk Up Authentication mode (a.k.a. “Log In At Walk Up”)

In the evaluated configuration, both Task-based Authentication mode and Walk Up Authentication mode must always be enabled simultaneously.

For the Control Panel Task-based Authentication mode, the TOE allows the administrator to choose which I&A mechanism is required for a given task (see FIA_UAU.1 for a list of Control Panel tasks). Therefore, task selection can be performed by the user before the Task-based I&A process starts. For example, a user would select the Print operation on the Control Panel and then be prompted to authenticate using the authentication mechanism defined for that task. Valid authentication values for Task-based Authentication are:

- User PIN
- LDAP
- Kerberos

For Control Panel Walk Up Authentication, the TOE allows the administrator to choose a single I&A mechanism which is required for all tasks (i.e. Home Screen Access). All users must first log into the hardcopy device before selecting a task. Valid authentication values for Walk Up Authentication are:

- User PIN
- LDAP
- Kerberos

Because both modes are enabled simultaneously in the evaluated configuration, the user must first log in through Walk Up Authentication and then select a task. If the Task-based Authentication method is different from the Walk Up Authentication method, then the user will also be required to log in using the Task-based Authentication method in order to perform the task. If the Walk Up Authentication method and Task-based Authentication method are the same, then the system will only perform the Walk Up Authentication.

Only an authorized administrator can configure the Control Panel Task-based and Walk Up authentication modes and only an authorized administrator can select the Control Panel authentication mechanisms used by the Control Panel to authenticate users.

This section maps to the following SFRs:

- FIA_ATD.1 (User Role)
- FIA_UAU.1
- FIA_UAU.2-walkup
- FIA_UID.1
- FIA_UID.2-walkup
- FIA_USB.1
- FMT_MOF.1-auth

7.2.1.1 Local I&A

7.2.1.1.1 User PIN Authentication

User PIN Authentication is only available through the Control Panel. The TOE contains a local user database for defining non-administrative (U.NORMAL) user accounts used to support the User PIN Authentication mechanism. Each user account contains the following security attributes:

- User PIN which is 8 digits (the number of digits is manually enforced by administrators)

The User PIN serves as both the user identifier and the authentication secret. Each user’s User PIN is unique from all other users. The accounts are created and managed through the Embedded Web Server (EWS) interface using the User PIN Authentication screen. Only the EWS interface can be used to set and modify the PIN of an account (i.e. users cannot change their own PINs). The accounts can only be used to log in through the Control Panel. No other interfaces will accept these accounts for I&A. All accounts are non-administrative accounts; thus, only non-administrative users can log in through the Control Panel. The TOE allows User PINs to be up to 8 digits, but administrators are required to create User PINs that are 8 digits in the evaluated configuration.

In addition to the SFRs mapped in section 7.2.1, this section maps to the following SFRs:

- FIA_ATD.1
- FMT_MTD.1-users

7.2.1.2 Remote I&A

The TOE supports the use of remote I&A mechanisms for Control Panel users (U.NORMAL). These mechanisms are only used by the Control Panel (i.e. they are not used by the PJL, HTTP/EWS, and SNMP interfaces). The following trusted operational environment mechanisms are supported by the TOE:

- LDAP
- Kerberos

In all cases, an authentication agent exists in the TOE which communicates with the U.ADMINISTRATOR specified remote I&A mechanism. The TOE receives authentication credentials from the Control Panel users (U.NORMAL) and, via the authentication agent, passes the credentials to the remote authentication mechanism in the IT Environment. The remote authentication mechanism returns an authentication decision to the TOE. This decision is then enforced by the TOE by granting or denying access to the Control Panel user.

In the case of LDAP, the user name and password entered at the Control Panel are used to bind to the LDAP server. The user must have a valid and active LDAP account in order to successfully bind using this method.

In the case of Kerberos, the user name and password entered at the Control Panel are used to authenticate with the Kerberos server. The user must have a valid and active Kerberos account in order to successfully bind using this method.

In addition to the SFRs mapped in section 7.2.1, this section maps to the following SFRs:

- none

7.2.1.3 Additional I&A Features

The TOE obscures authentication PINs and passwords typed into the Control Panel by displaying an asterisk for every character typed by the user.

This section maps to the following SFR:

- FIA_UAU.7

7.2.2 IPsec I&A

The TOE uses IPsec to mutually authenticate Network Client Computers, Administrative Computers, and Authenticated Server Computers. The TOE uses IP addresses and X.509v3 certificates via the IKE protocol to identify which computers are Network Client Computers, which are Administrative Computers, and to authenticate these computers. It also uses IP addresses and X.509v3 certificates via the IKE protocol to connect to the Authenticated Server Computers. Only an authorized administrator can configure the list of Network Client Computers, Administrative Computers, and Authenticated Server Computers. Mutual identification and authentication must be completed before any tasks can be performed by a Network Client Computer, an Administrative Computer, or an Authenticated Server Computer. (Authenticated Server Computers don’t perform tasks on the TOE; therefore, they are neither U.ADMINISTRATOR nor U.NORMAL users. Instead, the TOE is the client of the Authenticated Server Computers and performs tasks on the Authenticated Server Computers.)

The TOE uses IP addresses and the IPsec/Firewall to determine which connection requesting computers are Network Client Computers and which are Administrative Computers. Both types can access the PJL interface, but only Administrative Computers can access the HTTP/EWS interface and SNMP interface.

IP address management for identification is discussed in section 7.3.2. Certificate management is discussed in section 7.6.

This section maps to the following SFRs:

- FIA_ATD.1 (User Role, IP address)
- FIA_UAU.2-ipsec
- FIA_UID.2-ipsec
- FIA_USB.1

7.3 Data Protection and Access Control

7.3.1 Common Access Control

7.3.1.1 Job PIN and General Access

The TOE supports Job PIN-based access control. In the evaluated configuration, a Job PIN (Personal Identification Number) must be a 4 digit value selected by the user when creating a print job or a stored copy job. Job PINs are optional and, by default, do not exist on a print job or a stored copy job.

Job PINs are used to protect stored jobs from being printed and/or deleted by other users. Users logged in at the Control Panel can see a list of the print jobs and copy jobs stored in Job Storage (nonvolatile storage) on the system regardless of the user who created the jobs. The logged in users can print and/or delete any of the stored jobs that don't have a Job PIN associated with them and any stored job for which they do know the Job PIN.

A Job PIN can be assigned to a print job when submitting a print job from a Network Client Computer. It is up to the user to decide whether a Job PIN is required for the print job or not.

A Job PIN can be assigned to a stored copy job when the user creates the stored copy job. A stored copy job allows a user to copy a hardcopy document to Job Storage and print one or more copies of the document or delete the document at a later time.

Once a Job PIN is set on a job, it cannot be changed.

Administrators can delete the following types of Job Storage jobs, regardless of ownership, by having the TOE automatically delete the job after a specified time interval:

- Proof and hold print job
- Personal print job with or without a Job PIN
- Quick copy print job

(The above job types will also be deleted by turning off (rebooting) the TOE.)

Administrators can delete the following types of Job Storage jobs directly:

- Stored print job without a Job PIN
- Stored copy job without a Job PIN

Administrators cannot delete the following Job Storage jobs:

- Stored print job with a Job PIN
- Stored copy job with a Job PIN

Administrators can also restrict (modify) the use of color versus black & white (D.FUNC) when printing. Jobs requesting color can be limited to just black & white.

This section maps to the following SFRs:

- FDP_ACC.1-cac
- FDP_ACF.1-cac
- FMT_MSA.1-cac
- FMT_MSA.3-cac

7.3.1.2 Fax PIN (Receive Fax jobs)

The TOE assigns a Fax PIN (a.k.a. Fax Printing PIN) of the administrator's choosing to each Receive Fax job (D.DOC+FAXIN). This PIN prevents the automatic printing of each Receive Fax job and protects each Receive Fax job from unauthorized access. The Fax PIN can only be set by an administrator. In the evaluated configuration, administrators must set an 8 digit Fax PIN value as required by the TOE's guidance documentation.

Receive Fax jobs are stored in Job Storage in a folder called "Stored Faxes." A Receive Fax job is not printed until an authorized user enters the Fax PIN via the Control Panel for the selected Receive Fax job. An authorized user is any logged in Control Panel user (U.NORMAL) who knows the Fax PIN of the Receive Fax job. By controlling who has knowledge of the Fax PIN, an administrator can control who can print and delete Receive Fax jobs. Receive Fax jobs must be deleted manually (i.e. they are not automatically deleted by the TOE).

From both a conceptual and implementation perspective, the Fax PIN is a predefined Job PIN that is assigned by the TOE to each Receive Fax job in Job Storage. Because the Fax PIN is assigned to each Receive Fax job during the receiving process, changing the Fax PIN will only affect the PIN value of new Receive Fax jobs. Receive Fax jobs that exist prior to a Fax PIN change will retain the PIN value that was in effect at the time they were received.

If the fax “Archive to Email Address” functionality is enabled for incoming faxes, an email containing the fax is automatically sent to an administrator configured email address when the fax is received. Outgoing faxes can be archived to either an administrator configured fax number or to an administrator configured email address using the “Archive to Fax Number” or “Archive to Email Address” features, respectively, but not to both.

This section maps to the following SFRs:

- FDP_ACC.1-cac
- FDP_ACF.1-cac
- FMT_MSA.1-faxpin
- FMT_MSA.3-faxpin
- FMT_MTD.1-pins (Fax PIN)

7.3.1.3 Fax Polling Receive jobs

The Fax Polling Receive function (defined in Table 1-1) allows an authorized user (U.NORMAL) to request a fax from another fax device over the analog fax phone line from the Control Panel of the TOE. This is called a Fax Polling Receive job (D.DOC+FAXIN) by this document. The user must be authenticated via the Control Panel in order to perform this function.

Any faxes received from a polling request are immediately printed by the TOE and deleted. They are not stored in Job Storage. This implies that the user is the owner of these faxes, the user can read these faxes, and the user deletes these faxes. The user cannot modify these faxes. In addition, Fax Polling Receive jobs are not archived by the fax “Archive to Email Address” feature.

This section maps to the following SFRs:

- FDP_ACC.1-cac
- FDP_ACF.1-cac

7.3.1.4 PJL Password

Print jobs contain Printer Job Language (PJL) commands. Some of these commands have administrative capabilities and are, therefore, protected with a PJL Password by the TOE. In order to execute password protected PJL commands, the print job must contain the PJL Password.

The PJL Password must be 9 or more digits (enforced by the person setting the password). The password is managed through the PJL protocol using an administrative application like HP’s Web Jetadmin (part of the operational environment) or through the EWS interface. Administrators control which users (U.NORMAL) know the PJL Password, if any. Users who know the PJL Password can modify the password through the PJL protocol. The administrator must also know the PJL Password in order to modify it.

This section maps to the following SFRs:

- FDP_ACC.1-cac
- FDP_ACF.1-cac
- FMT_MSA.1-pjl
- FMT_MSA.3-pjl

7.3.2 TOE Function Access Control

The TOE controls access to TOE functions through the use of authentication mechanisms. These mechanisms require TOE users to authenticate themselves in order to perform TOE functions. The authentication process assigns a User Role to the authenticated user. The exception is the incoming analog fax connection which does not support an authentication mechanism since the fax protocol does not support authentication.

Network Client Computers, Administrative Computers, and Authenticated Server Computers are authenticated using IPsec and X.509v3 certificates. The TOE determines which systems are Network Client Computers and which systems are Administrative Computers based on each system's IP address. Administrators also configure the IP addresses of Server Computers. Administrators use the EWS interface to initialize and modify the set of allowed IP addresses. Administrators also manage the X509v3 certificate supported by the TOE.

This section maps to the following SFRs:

- FDP_ACC.1-tfac
- FDP_ACF.1-tfac
- FIA_ATD.1 (User Role, IP address)
- FMT_MSA.1-tfac
- FMT_MSA.3-tfac
- FMT_MTD.1-pins (IP addresses)

7.3.3 Residual Information Protection

7.3.3.1 Document Deallocation

When the TOE deletes an object defined in section 6.1.2.5, the contents of the object are no longer available to TOE users.

This section maps to the following SFR:

- FDP_RIP.1

7.3.3.2 Secure Storage Erase

In the evaluated configuration (Secure File Erase mode set to Secure Fast Erase or to Secure Sanitize Erase), the Secure Storage Erase feature enables administrators to delete (overwrite) all permanent data, user job-related data, and non-system data files from the hard drive on demand.

The TOE stores various types of files on its hard drive for various reasons. These files include permanent files, user job-related data files, and all other non-system data files. The files that are called permanent files include stored jobs, proof and hold jobs, disk-based fonts, and disk-based macros (forms). User job-related files include temporary image files that are required to complete Print jobs, Copy jobs, Send E-mail jobs, Send to Folder jobs, or Fax jobs. The TOE may also store other non-system data files on the hard drive. Secure Storage Erase overwrites all of these files and all other data, other than critical system variables, from the hard drive on demand by the administrator. During this process for the HCD hard drive, Secure Storage Erase uses the Secure File Erase mode (method) that is configured for the TOE to delete (destroy) the information.

Secure Storage Erase reboots the HCD. During this reboot, the HCD System Firmware skips mounting the storage device that is scheduled for the overwrite operation. This allows the Secure Storage Erase feature to have full access to the storage device. This also causes other HCD (and TOE) services to become unavailable during the operation. As the process continues, all sectors of the storage device that contain permanent, non-system, or user job-related data are overwritten. When overwriting is finished, the HCD reboots again to remount the storage device normally and to enable regular HCD operations.

If the HCD is turned off after beginning a scheduled Secure Storage Erase operation, the TOE will continue to attempt the operation until it is successful. If power to the HCD is lost during a Secure Storage Erase operation, the TOE will restart the Secure Storage Erase operation on reboot starting at the first block and continuing sequentially until completed.

This section maps to the following SFRs:

- FDP_RIP_EXP.3
- FMT_MOF.1-ripstore

7.3.3.3 Secure File Erase

With the Secure File Erase mode set to a secure mode, files that have been written to the hard drive during Print, Copy, Send E-mail, Send to Folder, or Fax operations are overwritten in real time when the TOE is finished processing the files.

The Evaluation Configuration requires the administrator to change the factory default Secure File Erase mode to either of the following options:

- Secure Fast Erase
- Secure Sanitizing Erase

Secure Fast Erase is the Secure File Erase mode by which all addressable file locations are overwritten once with a character. This mode provides sufficient security for most network environments.

Secure Sanitizing Erase is the Secure File Erase mode by which file locations are overwritten with three passes using a secure, repetitive method to remove all residual or remanent data as a file is deleted. The first pass is a character written to each byte of each deleted sector. The second pass is the complement of the first character written to each byte of each deleted sector. The third pass is a random character written to each byte of each deleted sector. This mode provides a higher level of security for sensitive network environments that require it.

This section maps to the following SFRs:

- FDP_RIP_EXP.3
- FMT_MOF.1-ripfile

7.4 Protection of the TSF

7.4.1 Restricted Forwarding of Data (including Fax Separation)

The TOE allows an administrator to enable / disable the forwarding of data received from an External Interface to the Shared-medium Interface. The terms External Interface and Shared-medium Interface are defined in [2600.2] and duplicated in section 1.2 of this Security Target. This implies that an administrator can configure the TOE to have a distinct functional separation between the analog fax phone line and the Shared-medium Interface (i.e. network interface). The administrator can disable the fax feature “Archive to Email Address” to prevent data and commands from being sent from the Public Switched Telephone Network (PSTN) to the local network.

This section maps to the following SFR:

- FPT_FDI_EXP.1

7.4.2 TSF Self-Testing

The TOE provides a set of self-tests for testing correct operation, TSF data integrity, and stored TSF executable code integrity. When the TOE boots, the bootloader performs integrity checks on the firmware executables prior to loading them into memory and notifies the Control Panel user if any checks fail.

The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of correct operations tests and TSF data integrity tests at the request of the administrator. The specific security related tests available to the administrator are listed in section 6.1.5.3. In some cases, the tests can only be executed if the system is configured to use the feature being tested. For example, in order to execute a User PIN authentication database related test, the TOE’s User PIN authentication mechanism must be enabled and configured by an administrator prior to running the test.

This section maps to the following SFR:

- FPT_TST.1

7.4.3 Reliable Timestamps

The TOE contains a system clock that is used to generate reliable timestamps. Only administrators can manage the system clock.

This section maps to the following SFR:

- FPT_STM.1

7.5 TOE Access Protection

7.5.1 Inactivity Timeout

The TOE supports an inactivity timeout for Control Panel logins. If a logged in user is inactive for longer than the specified period, the user is automatically logged off of the system. The inactivity period is managed by an authorized administrator through the EWS interface. Only one inactivity period exists per TOE.

This section maps to the following SFR:

- FTA_SSL.3

7.6 Trusted Channel Communication

Shared-medium communications (i.e. non-fax connections) between the TOE and other devices use a trusted channel mechanism to protect the communications from disclosure and modification. The following table provides a list of the mechanisms used to protect these channels.

Table 7-1 - Trusted channel connections

Secure Protocol	Functions Supported
IPsec	The following functions use this protocol to provide trusted channel: • all PJL requests from Network Client Computers and Administrative Computers – these connections are initiated by Network Client Computers and Administrative Computers • all Send E-mail connections (i.e. SMTP gateway) – these connections are initiated by the TOE • all Send to Folder connections (i.e. FTP, CIFS) – these connections are initiated by the TOE • all HTTP/EWS connections (including web browser, DSMP, and certificate upload) – these connections are initiated by Administrative Computers • all SNMP connections – these connections are initiated by Administrative Computers • all LDAP connections (i.e. LDAP remote authentication) – these connections are initiated by the TOE • all syslog server connections – these connections are initiated by the TOE
Kerberos	The following functions use the protocol to provide trusted channel: • all Kerberos connections (i.e. Kerberos remote authentication) – these connections are initiated by the TOE

IPsec uses X.509v3 certificates to protect communications. In the evaluated configuration, the supported IPsec encryption and message digests are:

- AES-128
- SHA-1

Kerberos uses the Kerberos defined mechanism which includes a Kerberos encryption password/key to protect the communications. In the evaluated configuration, the supported Kerberos encryption and message digests are:

- AES-128, AES-256, 3DES
- SHA-1, MD5

The TOE maintains two certificates for IPsec:

- Jetdirect certificate

- Certificate Authority (CA) certificate

The Jetdirect certificate identifies the TOE and provides cryptographic keys for the TOE. The CA certificate allows the TOE to validate the certificates of connecting computers.

The HTTP interface allows authorized administrators to manage, via the certificate upload request, the X.509v3 certificates used by IPsec. This interface allows the Jetdirect certificate to be overwritten with a new certificate. It also allows the CA certificate to be added or deleted. In the evaluated configuration, the self-signed Jetdirect certificate provided with the system must be replaced and a CA certificate must be added. (The generation and distribution of certificates are not performed by the TOE and are considered part of the operational environment.)

SNMPv1 and SNMPv2c are limited to read-only interfaces in the evaluated configuration, meaning that these interfaces cannot be used to modify information controlled by the TOE. SNMPv3 can be used to modify information.

The TOE can initiate communication via the trusted channel as required by FTP_ITC.1.3. For example, the Send E-mail and Send to Folder connections, which are initiated by the TOE, transfer D.DOC and D.FUNC information in the form of scanned objects. The LDAP connection, which is initiated by the TOE, transfers D.PROT and D.CONF information in the form of user passwords.

This section maps to the following SFRs:

- FMT_MTD.1-certs
- FTP_ITC.1

7.7 Management

The TOE supports the following types of users:

- Administrators (U.ADMINISTRATOR)
- Users (U.NORMAL)
- Authenticated Servers (U.SERVER)
- Nobody (See [2600.2])

Administrators maintain and configure the TOE and operating environment. Users perform the standard print, copy, fax, etc. functions on the system. Authenticated Servers are computers that are contacted and authenticated by the TOE to perform services on behalf of the TOE, such as SMTP gateway and LDAP.

This section maps to the following SFRs:

- FMT_SMF.1
- FMT_SMR.1

8 Abbreviations

CCEVS	Common Criteria Evaluation and Validation Scheme
CIFS	Common Internet File System
DSMP	Digital Sender Module Protocol
EWS	Embedded Web Server
FTP	File Transfer Protocol
HCD	Hardcopy Device
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IPsec	Internet Protocol Security
MFP	Multifunction Product
NIAP	National Information Assurance Partnership
PIN	Personal Identification Number
PJL	Printer Job Language
PML	Printer Management Language
PSTN	Public Switched Telephone Network
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation
XML	Extensible Markup Language