Hewlett-Packard LaserJet M4555 MFP Series and Color LaserJet CM4540 Series with Jetdirect Inside Security Target

Version:	**2.0**
Status:	**Final**
Last Update:	**2014-01-22**

Trademarks

The following term is a trademark of atsec information security corporation in the United States, other countries, or both:

- atsec®

The following terms are trademarks of The Institute of Electrical and Electronics Engineers, Incorporated in the United States, other countries, or both:

- 2600.2™
- IEEE®

The following term is a trademark of Massachusetts Institute of Technology (MIT) in the United States, other countries, or both:

- Kerberos™

The following terms are trademarks of Microsoft Corporation in the United States, other countries, or both:

- Microsoft®
- Windows®

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.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
2.0	2014-01-22	King Ables, atsec	Final.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	Hewlett-Packard LaserJet M4555 MFP Series and Color LaserJet CM4540 Series with Jetdirect Inside Security Target
Version:	2.0
Status:	Final
Date:	2014-01-22
Sponsor:	Hewlett-Packard Development Company, L.P.
Developer:	Hewlett-Packard Development Company, L.P.
Certification Body:	CSEC
Certification ID:	CSEC2012003
Keywords:	Hewlett-Packard, HP, Color LaserJet, LaserJet, CM4540, M4555, multifunction product, MFP, hardcopy device, HCD, Printer, Jetdirect Inside, separation of analog fax from network.

1.2 TOE Identification

The TOE is the Hewlett-Packard LaserJet M4555 MFP Series and Color LaserJet CM4540 Series with Jetdirect Inside.

1.3 TOE Type

The TOE type is the internal firmware providing the functionality of a multifunction product (MFP, e.g., fax, copier, printer, scanner).

1.4 TOE Overview

The Hewlett-Packard LaserJet MFPs are enterprise network multifunction products designed to be shared by many client computers and users. These products are designed to meet the requirements of the [PP2600.2] protection profile in conjunction with [CCEVS-PL20] in the environment defined by these two documents (the Policy Letter modifies the requirements and environment).

MFPs contain functions for the copying, faxing, printing, and scanning of documents. These hardcopy devices (HCDs), as they are called in [PP2600.2], are self-contained units that include processors, memory, networking, a hard drive, an image scanner, and a print engine. Two operating systems, two web servers, and HCD applications reside within the firmware of the HCD. The TOE is the contents of the firmware with the exception of the operating systems, which are part of the Operational Environment.

The HCD models for which the firmware is evaluated are listed in the following table along with the evaluated firmware version numbers for each model:

TOE Name	TOE Version
HP Color LaserJet CM4540 MFP Series	MFP Firmware version: 2204045_233099 Jetdirect Inside version: JDI22210024.FF

TOE Name	TOE Version
HP LaserJet M4555 MFP Series	MFP Firmware version: 2204045_233103 Jetdirect Inside version: JDI22210024.FF

Table 1: TOE Reference

Each model 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 and automatic logout)
- Trusted channel communication and certificate management
- User and access management

1.4.1 Intended method of use

[PP2600.2] is defined for a commercial information processing environment in which a moderate level of document security, network security, and security assurance are required.

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

The HCDs 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. One HCD is managed by one designated administrative computer. The HCDs are not intended be connected to the Internet.

Analog fax phone lines can be connected to the HCDs 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 firmware of the HCD and it also supports external/remote Windows authentication (via Kerberos) and Lightweight Directory Access Protocol (LDAP) authentication servers to identify and authenticate users.

The evaluated configuration supports the HP Web Jetadmin administrative application for managing the TOE. This HCD application uses the Hypertext Transfer Protocol (HTTP), Hypertext Markup Language (HTML), Simple Object Access Protocol (SOAP), Extensible Markup Language (XML), Open Extensibility Platform device layer (OXPd), Printer Job Language (PJL), and Simple Network Management Protocol (SNMP) to communicate to the HCD. (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 and faxes remotely. It also can receive encrypted jobs to protect the job contents while stored in the HCD.

The HCD does support a Universal Serial Bus (USB) port for document input and firmware updates, but its use is disallowed in the evaluated configuration.

1.5 TOE Description

1.5.1 TOE architecture

As mentioned previously, the TOE is the firmware of an enterprise network multifunction printer 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 embedded Jetdirect Inside print server's built-in Ethernet, to an analog phone line using its internal analog fax modem, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration).

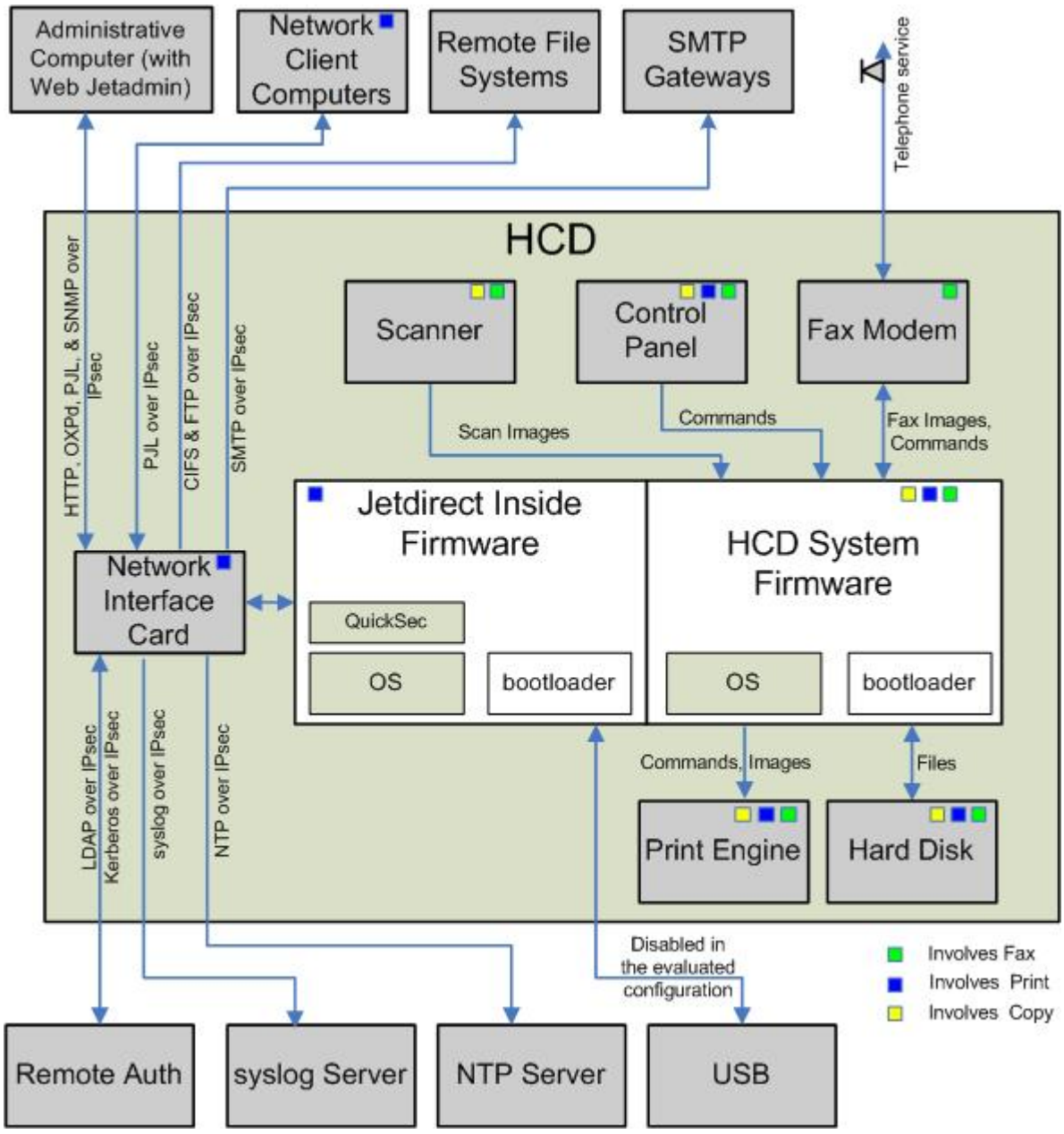

Figure 1: HCD physical diagram

Figure 1 shows a high-level physical diagram of an HCD with the unshaded areas representing the TOE and the shaded areas indicating components that are part of the Operational Environment.

At the top of this figure is the Administrative Computer which connects to the TOE using Internet Protocol Security (IPsec) with X.509v3 certificates for both mutual authentication and for protection of data from disclosure and alteration. This computer can administer the TOE using the following interfaces over the IPsec connection:

- Embedded Web Server (EWS)

- Web Services layer
- Printer Job Language (PJL) via TCP port 9100
- Simple Network Management Protocol (SNMP)

The HTTP-based EWS administrative interface allows administrators to remotely manage the features of the TOE using a web browser.

The Web Services layer allows administrators to manage the TOE using HP's Web Jetadmin application, which is part of the operating environment. Web Services supports both HP's Open Extensibility Platform device (OXPd) protocol and certain WS* web services (defined by w3.org) accessed via the Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML) protocols.

Printer Job Language (PJL) can be sent to the HCD multiple ways. In the evaluated configuration, the methods are limited to EWS and directly on TCP port 9100. For the purposes of this Security Target, we define the PJL Interface as PJL data sent to port 9100. The PJL Interface allows administrators to manage protected data by password protecting the administrative commands of PJL with the PJL Password.

The SNMP network interface allows administrators to remotely manage the TOE using SNMP-based administrative applications like the HP Web Jetadmin application.

Web Jetadmin uses the HTTP, OXPd, PJL, SOAP/XML, and SNMP protocols to manage the TOE. Remote applications such as web browsers and Web Jetadmin are part of the Operational Environment, not part of the TOE.

The TOE protects all network communications with Internet Protocol Security (IPsec), which is part of the embedded Jetdirect Inside print server. Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using X.509v3 certificates. An identity certificate for the HCD must be created outside the TOE, signed by a Certificate Authority (CA), and imported into the TOE with the Certificate Authority's CA certificate.

Because IPsec authenticates the computers (IPsec authenticates the computer itself; IPsec does not authenticate the individual users of the computer), access to the Administrative Computer 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 the Administrative Computer and Network Client Computers by using IP addresses, IPsec, and the embedded Jetdirect Inside print server's internal firewall. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one and the Device Administrator Password must be set.

The TOE can also communicate with Authenticated Server Computers using IPsec.

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. Because the fax protocol doesn't support authentication of incoming analog fax phone line users, anyone can connect to the analog fax phone line (unless the number has been added to the Blocked Fax Numbers list), but the only function an incoming fax phone line user can perform is to transmit a fax to the HCD.

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 HCD to retrieve faxes from other fax devices. This is called a Fax Polling Receive job by this document. To perform this function, the user authenticates via the Control Panel of the HCD and initiates the function by entering the phone number of the other fax device. The HCD 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 HCD does not accept polling requests from other fax devices (i.e., the HCD does not support the Fax Polling Send functionality).

The TOE protects stored jobs with either a 4-digit Job PIN or by accepting (and storing) an encrypted job from a user computer. Both protection mechanisms are optional by default and are mutually exclusive of each other if used. In the evaluated configuration, every job must either be assigned a 4-digit Job PIN or be an encrypted job.

The TOE also supports remote file systems for the storing of scanned documents and faxes. 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 product is capable of encrypting stored document files according to the Adobe PDF specification.

The TOE can be used to email scanned documents or received faxes. 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 product is capable of encrypting email according to the S/MIME specification. The TOE can only protect unencrypted 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.

The TOE supports both local and remote authentication mechanisms. The local mechanism is called Local Device authentication which supports individual user accounts. The user account information is maintained in the Local Device authentication database within the HCD. Remote authentication uses both LDAP and Windows authentication (Kerberos). The TOE uses IPsec with X.509v3 certificates to protect both LDAP and Kerberos communications.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of a touch sensitive LCD screen and several physical buttons that are attached to the HCD. It is the device interface that a user uses to communicate to the HCD 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. When a user signs in at the Control Panel, a Permission Set is associated with their session which determines the functions the user is permitted to perform.

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

The HP Secure Hard Disk (a.k.a. hard drive) provides hardware-based encryption and persistent storage to securely manage sensitive print, copy, scan, and fax data. Data on the hard disk is always encrypted and the encryption key is locked to the device. Encryption is transparent to the device

and the user. 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 by generating and forwarding audit records to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between the HCD and the syslog server and to mutually authenticate the HCD and syslog server.

The Jetdirect Inside Firmware and HCD System Firmware components comprise the firmware on the system. They are shown as two separate components and run in separate operating systems. Both firmware components also contain a bootloader (to boot their respective operating systems) and an Embedded Web Server (EWS). While each operating system is included in the firmware, both operating systems are outside of the TOE (in the Operational Environment).

Both the Jetdirect Inside Firmware and HCD System Firmware are contained by and executed on their own customized processors. Each processor is connected to a shared I/O processor which provides access to the hard drive, the Control Panel, and the Scanner processor. None of the processors are included in the TOE, all hardware is in the Operational Environment.

The Jetdirect Inside firmware includes SNMP, IPsec, a firewall, and the management functions for managing these network-related features. The Jetdirect Inside firmware also provides the network stack and drivers controlling the HCD's Ethernet interface.

The HCD System Firmware controls the overall functions of the TOE from the Control Panel to the hard drive to the print jobs.

Table 2 shows the main HCD supported functions available to a normal user (defined as U.NORMAL in [PP2600.2]) and the terminology used in the HCDs' guidance documentation.

	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**	**HTTP**	**HP LaserJet Terminology**
Scan	X						X							Stored Copy Job (requires 4-digit Job PIN)
	X									X				Email
	X										X			Save to Network Folder
	X											X		Save to FTP Server
	X												X	Save to HTTP
Copy	X					X								Copy Job, Color Copy Job

	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**	**HTTP**	**HP LaserJet Terminology**
Print		X					X							Stored Job, Personal Job
				X		X								Print from Job Storage (Job PIN required in the evaluated configuration)
					X	X								Print Fax
Fax In			X					X						Receive Fax
			X			X								Fax Polling Receive
			X						X					Fax Forwarding
			X							X				Archive to Email Address
			X								X			Archive to Network Folder
			X									X		Archive to FTP Server
Fax Out	X								X					Send Fax
	X									X				Archive to Email Address
	X										X			Archive to Network Folder
	X											X		Archive to FTP Server

Table 2: HCD terminology for user functions

Some job types can be set to provide notification when completed. The default setting is no notification, alternate settings notify on any job completion (success or failure) or on failure only. Notification can be made via a printed page or an email message to the user.

In the evaluated configuration, the job types for which notification may be set are:

- sending a fax
- archiving to email
- saving a job to a network folder (shared folder or FTP server)

Figure 2 shows the HCD boundary in grey and the firmware (TOE) boundary in blue (the TOE being comprised of the HCD System firmware and the Jetdirect Inside firmware excluding the underlying operating systems). The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the HCD System firmware. The HCD System firmware and Jetdirect Inside firmware each contain an operating system (which is part of the Operational Environment, not the TOE) and a customized bootloader to start the operating system. The HCD System firmware also includes HCD applications that drive the functions of the TOE. Both firmware components work together to provide the security functionality defined in this document for the TOE. (PSTN is an abbreviation for Public Switched Telephone Network.)

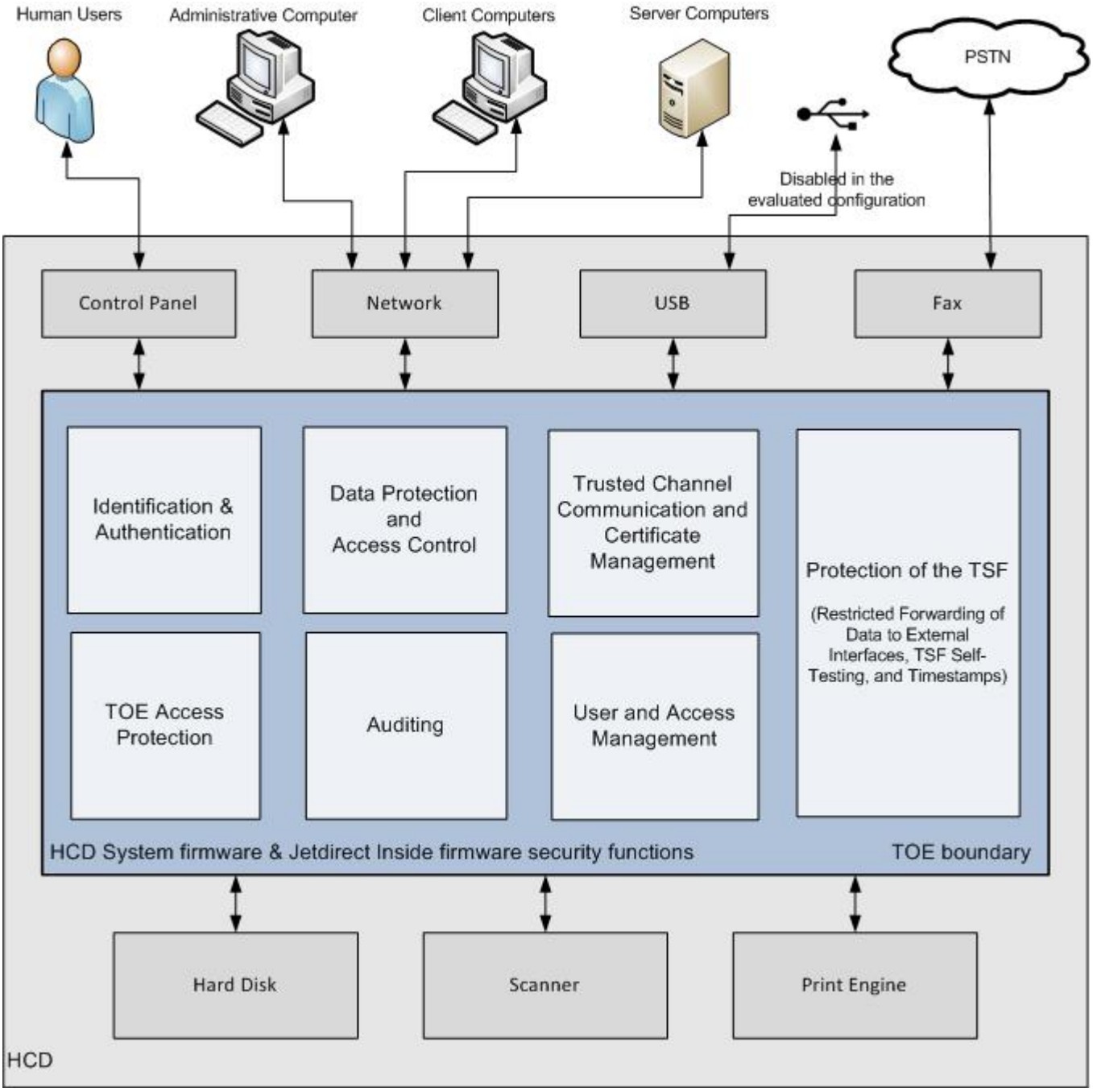

Figure 2: HCD logical diagram

1.5.2 TOE security function (TSF) summary

1.5.2.1 Auditing

The TOE performs auditing of security relevant functions. Both the Jetdirect Inside and HCD System firmware generate audit records. The TOE connects and sends audit 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 and authentication

1.5.2.2.1 Control Panel I&A

All HCDs have a Control Panel used to select a function to be performed, such as Print, Copy, Scan, or Fax. The Control Panel supports both local and remote authentication.

The mechanism for local authentication, which is part of the TOE firmware, is called:

- Local Device Sign In

Remote authentication mechanisms used by the TOE are:

- LDAP Sign In
- Windows Sign In (via Kerberos)

For successful remote authentication, Control Panel users must enter their username and password as defined for the remote authentication mechanism.

Prior to signing in, the user may select a sign in method, sign in, or get help on various printer functions. All users must sign in before being presented with the home screen allowing access to printer functions.

When users authenticate through the Control Panel, the HCD displays asterisks for each character of a PIN, Access Code, 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 HCDs to submit print jobs and to manage the HCDs. HCDs use IPsec to mutually authenticate computers that attempt to connect to them over the following interfaces:

- EWS (HTTP)
- Web Services (OXPd and SOAP/XML)
- PJL
- 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 HCDs are classified as either Network Client Computers or Administrative Computers. HCDs use IP addresses and the internal firewall to determine which computers are Network Client Computers and which one is the Administrative Computer.

The Administrative Computer is allowed to connect to all interfaces listed above, whereas Network Client Computers are limited to only the PJL Interface (TCP port 9100).

Because IPsec mutual authentication is performed at the computer level, not the user level, the computer allowed to access the TOE via EWS, OXPd, SOAP/XML, and SNMP must itself be the Administrative Computer. This means that non-TOE administrative users should not be allowed to logon to the Administrative Computer because every user of the Administrative Computer is potentially a TOE administrator.

In addition, HCDs 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 these 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 Permission Sets

Each task performed by the TOE requires one or more permission. These permissions are defined in Permission Sets (aka User Roles). The applied permission set can be a combination of various permission sets associated with a user. The default Permission Sets in the evaluated configuration are:

- Device Administrator (assigned to U.ADMINISTRATOR)
- Device User (assigned to U.NORMAL)

The product includes a Guest Permission Set, but it has no permissions in the evaluated configuration. It also includes a Service Permission Set which can only be used in conjunction with the Service PIN, but the Service PIN is disallowed in the evaluated configuration. Additional (custom) Permission Sets can be created and applied by the administrator.

The Device Administrator Permission Set has more permissions enabled than the Device User Permission Set. For example, the Device Administrator Permission Set has a fax permission enabled which allows a U.ADMINISTRATOR user to print incoming fax jobs stored in Job Storage. The Device User Permission Set has this permission disabled by default; therefore, the TOE denies a U.NORMAL user permission to print an incoming fax job stored in Job Storage.

Permission Set data is stored in the HCD and managed via EWS.

1.5.2.3.2 Job PINs

Users control access to print and stored copy jobs that they place on the HCD by assigning Job PINs to these jobs (required in the evaluated configuration). Job PINs must be 4 digits in length. Job PINs limit access to these jobs while they reside on the HCD and allows users to control when the jobs are printed so that physical access to the hard copies can be controlled.

1.5.2.3.3 Job Encryption Password

The TOE can store and decrypt encrypted stored print jobs received from a client computer which has the HP Universal Print Driver installed. A stored print job is first encrypted by the client computer using a user-specified Job Encryption Password. The job is then sent encrypted to the TOE and stored encrypted by the TOE. To decrypt the job, a Control Panel user must enter the correct Job Encryption Password used to encrypt the job.

1.5.2.3.4 PJL Password

The HCDs support 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.

1.5.2.3.5 Common access control

The TOE protects each non-fax job in Job Storage from non-administrative users through the use of a user identifier and either a Job PIN or a Job Encryption Password. The user identifier for a print job received from a client computer is either assigned by that client computer or assigned by the user sending the print job from the client computer. In the case of an encrypted print job, the user ID is assigned by the HP Universal Print Driver as obtained from Windows. For all other types of jobs, the user identifier is assigned by the TOE. Every non-fax job in Job Storage is assigned either a Job PIN or a Job Encryption Password by the user at job creation time.

The default rules for a non-administrative (U.NORMAL) user for accessing a non-fax job in Job Storage are:

- if the job is Job PIN protected:
  - the job owner (i.e., the authenticated user who matches the job's user identifier) can access the job without supplying the Job PIN
  - any non-owner authenticated user who supplies the correct Job PIN can access the job
- if the job is Job Encryption Password protected, any authenticated user who supplies the correct Job Encryption Password can access the job

By default, a Control Panel administrator (U.ADMINISTRATOR) user has a permission in their Permission Set that allows them to delete Job Storage jobs.

The TOE protects each fax job in Job Storage through the Permission Set mechanism. A user must have a specific fax permission in their Permission Set to access incoming fax jobs stored in Job Storage.

1.5.2.3.6 TOE function access control

For Control Panel users, the TOE controls access to certain Control Panel functions using a combination of Permission Sets and authentication databases. Permission Sets act as User Roles to determine if the user can perform a function controlled by permissions. In addition, the administrator can assign a specific authentication database to one or more Control Panel functions that require the user to authenticate against a specified authentication database in order to use those functions; otherwise, access by the user to those functions is denied by the TOE.

For IPsec users, the TOE uses the IP address of the connecting computer to determine the User Role of the computer (i.e., to determine if the computer is the Administrative Computer or a Network Client Computer). X.509v3 certificates are used in conjunction with the IP address to determine TOE function access.

1.5.2.4 Protection of the TSF

1.5.2.4.1 Restricted forwarding of data to external interfaces

The TOE allows an administrator to restrict the forwarding of data received from an External Interface to the Shared-medium Interface. Specifically, the fax features Fax Forwarding and Fax Archive, which can automatically forward or archive received faxes 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. In the evaluated configuration, the TOE synchronizes the system clock with a Network Time Protocol (NTP) server.

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.

1.5.2.5.2 Automatic logout

The Control Panel supports an administrator selectable automatic logout which logs the user out after their job is started. If the user logs in and never starts a job, the inactivity timeout feature will terminate the session.

1.5.2.6 Trusted channel communication and certificate management

The TOE supports IPsec to protect data being transferred over the Shared-medium Interface. IPsec uses X.509v3 certificates to authenticate the Network Client Computer, Administrative Computer, SMTP gateway, EWS (HTTP), Web Services (OXPd and SOAP/XML), PJL, SNMP, LDAP, NTP, and remote file system interfaces.

The TOE uses a software-based random number generator when creating symmetric encryption keys used as communications session keys and secret keys used during data integrity verification.

In addition, the TOE provides certificate management functions used to import X.509v3 certificates.

1.5.2.7 User and access management

The HCDs provide management capabilities for managing the functionality of each HCD. The HCDs provide management capabilities for managing the functionality of each HCD. The HCDs support the following roles:

- administrators (U.ADMINISTRATOR)
- users (U.NORMAL)
- authenticated servers (U.SERVER.AUTHD)

Administrators have the authority to manage the security functionality of the HCDs and to manage users. Users can only manage user data that they have access to on the HCDs. 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

The physical boundary of the TOE is the programs and data stored in the firmware of the HCD (except for the embedded operating systems) and the English-language guidance documentation.

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 (such as the processor board) are more difficult to access 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).

Because of the restricted access to the hard drive, the hard drive is considered a non-removable nonvolatile storage device from the perspective of [PP2600.2].

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

IPsec and the internal firewall are implemented in the firmware and are part of the TOE. All cryptographic operations used by IPsec in the evaluated configuration are implemented by the QuickSec cryptographic library which is part of the Operational Environment; therefore, the cryptographic operations used by IPsec are performed by the Operational Environment. The QuickSec library version 5.1 ([QuickSec51]), relied upon by the TOE, has been tested by the developer, SafeNet, Inc. The QuickSec library is outside the TOE scope, and is not covered by the evaluation.

Regarding the 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).

The following components are considered part of the Operational Environment and, therefore, beyond the scope of this evaluation:

- X.509v3 certificate and certificate request generation
- HP Web Jetadmin administrative tool
- HP Printer Drivers for client computers (for submitting print job requests from Network Client Computers)
- IPsec cryptographic operations accessed from the QuickSec library
- Kerberos server
- LDAP server
- NTP server
- remote file systems
- SMTP gateway
- syslog server
- web browser

- embedded operating system(s)

1.5.3.2 Logical

The TOE provides the following functions to the HCD owner:

- HCD management
- Control Panel interface
- network access
- access to internal hard drive
- scanner engine
- print engine
- copy function (scan + print)
- fax capability
- user functions listed in Table 2
- cryptographic functions required to decrypt an encrypted job
- cryptographic functions required by IPsec implemented in the QuickSec cryptographic library in the Operational Environment

The security functionality provided by the TOE has been described above and include:

- auditing
- identification and authentication
- data protection and access control
- trusted channel communications
- TOE Access protection

1.5.3.3 Evaluated configuration

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

- Secure Hard Disk must be configured with a password to activate hard drive encryption
- Device Administrator Password must be set
- Only one Administrative Computer is used to manage the TOE
- Third party applications cannot be installed on the HCD
- All jobs must be assigned a Job PIN or encrypted with a password
- PC Fax Send disabled
- Type A and B USB ports disabled
- Remote Firmware Upgrade through any means other than EWS (e.g., USB or PJL) disabled
- Jetdirect Inside management via telnet and 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)
- IPsec Authenticated Headers (AH) are disabled
- Full Authentication enabled (this disables the Guest account)
- SNMP support limited to:

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

- The Service PIN, used by a customer support engineer to access functions available to support personnel, must be disabled.

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 [PP2600.2] and is duplicated here so that readers won't have to read [PP2600.2] 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 3.

Designation	Definition	
U.USER	Any authorized User. Authorized Users are U.ADMINISTRATOR, U.NORMAL, and U.SERVER.AUTHD.	
	Designation	**Definition**
	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). A password must be set for all U.ADMINISTRATOR accounts in the evaluated configuration.
	U.SERVER.AUTHD	A User (trusted IT product entity) that the TOE authenticates and uses to provide additional services.

Table 3: Users

For the purpose of clarity in this Security Target, the following distinctions are made:

- **Control Panel users** – U.NORMAL and U.ADMINISTRATOR users who physically access an HCD's Control Panel.
  - **Security attributes**: User Role and User Identifier
- **Incoming analog fax phone line users** – Unauthenticated entities that initiate and transmit faxes to the HCD 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 HCD's PJL Interface (TCP port 9100) using IPsec and mutual authentication. The HCDs will accept print jobs from any user of a computer where the computer has successfully authenticated with the HCD.
    - **Security attributes:** User Role (defined by IP address)
- **Administrative Computers** – Computers (U.ADMINISTRATOR entities) that can successfully authenticate to the HCD's administrative interfaces (e.g., EWS/HTTP, SOAP/XML, SNMP) using IPsec and mutual authentication. An Administrative Computer may also connect to the HCD as a Network Client Computer (i.e., the Administrative Computer can send print jobs as a U.NORMAL user through the PJL Interface on port 9100).
    - **Security attributes:** User Role (defined by IP address)
- **Authenticated Server Computers** – Computers that provide services to the HCD. All server computers are U.SERVER.AUTHD entities and are successfully authenticated by the HCD using mutual authentication in IPsec. HCDs connect 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)
    - Kerberos servers
    - LDAP servers
    - NTP servers
    - SMTP gateways
    - syslog servers

  Non-authenticated servers are not permitted in the evaluated configuration.
    - **Security attributes:** User Role (defined by 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

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 HCD while processing an original document and printed hardcopy output.

Designation	Definition
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

Table 4: User Data

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 jobs** – Print jobs from a client computer that are stored in Job Storage. In the evaluated configuration, such jobs must 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 HCD is turned off (configurable by the administrator) or after an administrator specified time interval.
  - **Stored jobs** – Print jobs such as a personnel form, time sheet, or calendar from a client computer that are stored indefinitely on the HCD and reprinted. In the evaluated configuration, such jobs must be PIN protected with a Job PIN. For PIN protected stored jobs, the user must know the Job PIN (or have administrator privileges) in order to delete the job.
  - **Encrypted stored print jobs** – Print jobs like those described above but that require higher than normal protection (for example, documents containing company or employee confidential information). These jobs will be assigned a password by the submitter when submitted to the TOE. The user must know the password of the job in order to print or delete it. The administrator may delete it without knowing the password.
- **Email jobs** – Scan jobs that are scanned directly into an email and sent from the TOE to an SMTP gateway.
- **Save to Network 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 HCD. Stored copy jobs are scanned using the HCD scanner. In the evaluated configuration, users are required to protect Stored Copy jobs with a 4-digit Job PIN. The user must be the job owner, know the Job PIN of the job, or be an administrator in order to delete the job. .

A user signed in at the Control Panel will be the owner of any created stored copy job. Ownership of a print job sent from a client computer is defined as the username associated with the job when it is submitted to the HCD. The username is specified outside of the TOE, in the Operational Environment, so it can neither be confirmed nor denied by the TOE.

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.

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.

Table 5: TSF Data

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

TSF Data	D.CONF	D.PROT
Audit records	X	
Cryptographic keys and certificates	X	
Device and network configuration settings		X
Job data including Job PINs	X	
PJL Password	X	
PJL protocol excluding the PJL Password, job data, and Job PINs		X
Permission Sets		X
System time		X
User and Administrator identification data		X
User and Administrator authentication data	X	

Table 6: TSF Data Listing

1.5.4.3 SFR package functions

Functions perform processing, storage, and transmission of data. The following [PP2600.2]-defined functions apply to this Security Target.

Designation	Definition
F.CPY	Copying: a function in which physical document input is duplicated to physical document output

Designation	Definition
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

Table 7: SFR package functions

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 [PP2600.2]-defined attributes apply to this Security Target.

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.

Table 8: SFR package attributes

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL2, augmented by ALC_FLR.2.

This Security Target claims conformance to the following Protection Profiles and PP packages, if any:

- [PP2600.2]: IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20) . Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-CPY]: SFR Package for Hardcopy Device Copy Functions. Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-DSR]: SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions. Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-FAX]: SFR Package for Hardcopy Device Fax Functions. Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-PRT]: SFR Package for Hardcopy Device Print Functions. Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-SCN]: SFR Package for Hardcopy Device Scan Functions. Version 1.0 as of December 2009; demonstrable conformance.
- [PP2600.2-SMI]: SFR Package for Hardcopy Device Shared-medium Interface Functions. Version 1.0 as of December 2009; demonstrable conformance.

Common Criteria [CC] version 3.1 revision 4 is the basis for this conformance claim.

2.1 Protection Profile tailoring and additions

2.1.1 IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20) ([PP2600.2])

This protection profile is listed on the NIAP web site as a NIAP Approved Protection Profile (see http://www.niap-ccevs.org/cc-scheme/pp/) and tailored with NIAP CCEVS Policy Letter #20 ([CCEVS-PL20]). Questions regarding this tailoring should be addressed to NIAP.

Although the HCDs in this Security Target contain a nonvolatile storage device (i.e., a hard drive), this device is considered an internal, built-in component of the HCDs and, therefore, constitutes a non-removable nonvolatile storage device from the perspective of [PP2600.2] and [CCEVS-PL20]. 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 [PP2600.2].

The following tables provide the mappings of and rationale for how the SFRs in this Security Target map to the SFRs in the protection profile [PP2600.2]. The term “n/a” means “not applicable”.

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
FAU_GEN.1	FAU_GEN.1			The ST's FAU_GEN.1 combines the contents of FAU_GEN.1 from the common [PP2600.2] and FAU_GEN.1 from the [PP2600.2] 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 [PP2600.2] and the FDP_ACC.1's from the [PP2600.2] 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 [PP2600.2] and the FDP_ACF.1's from the [PP2600.2] 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	X	X	The TOE's Control Panel supports authentication (FIA_UAU.1) and the TOE supports IPsec authentication

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
				(FIA_UAU.2). The IPsec authentication complies with the more restrictive FIA_UAU.2.
FIA_UID.1	FIA_UID.1, FIA_UID.2	X	X	The TOE's Control Panel supports identification (FIA_UID.1) and the TOE supports IPsec identification (FIA_UID.2). The IPsec authentication complies with the more restrictive FIA_UID.2.
FIA_USB.1	FIA_USB.1			n/a
FMT_MSA.1(a)	FMT_MSA.1-perm and 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-perm and FMT_MSA.1-tfac	X		FMT_MSA.1(b) was further iterated because the operations differ.
FMT_MSA.3(a)	None			FMT_MSA.3(a) was omitted because the security attributes do not have default values in the evaluated configuration.
FMT_MSA.3(b)	None			FMT_MSA.3(b) was omitted because the security attributes do not have default values in the evaluated configuration.
FMT_MTD.1.1(a)	FMT_MTD.1-auth			The iteration name was changed from "(a)" to "-auth" (TSF Data associated with authorization) for better understandability when reading the ST.
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

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
FPT_STM.1	FPT_STM.1			When the TOE is configured to use its internal time source, then FPT_STM.1 applies. When the TOE is configured to use NTP, then A.NTP.RELIABLE and OE.NTP.RELIABLE apply.
FPT_TST.1	FPT_TST.1			n/a
FTA_SSL.3	FTA_SSL.3			n/a

Table 9: SFR mappings between 2600.2 and the ST

These SFRs in the Security Target are not required by and do not map to the protection profile [PP2600.2].

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
	FCS_CKM.1-ipsec-aes, FCS_CKM.1-ipsec-hmacsha1, FCS_CKM.2-ipsec-ikev1, FCS_CKM.2-ipsec-ikev2	X		FCS_CKM.1 iterations specify the types of cryptographic keys generated by the TOE for use with AES and HMAC in IPsec. FCS_CKM.2 iterations specify the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec.
	FCS_COP.1-ipsec-aes, FCS_COP.1-ipsec-rsa, FCS_COP.1-ipsec-hmacsha1	X		FCS_COP.1 iterations specify the AES encryption and decryption algorithm, the RSA decryption algorithm, and the HMAC algorithm used by the TOE in IPsec.
	FDP_ITC.1			The TOE can import a digital certificate that is used to authenticate an IPsec connection which provides a trusted channel for communication of data over Shared-medium Interfaces.
	FIA_SOS.1			FIA_SOS.1 specifies the password/PIN strength of certain authentication mechanisms used by the TOE.

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
	FIA_UAU.7			The TOE masks Job PINs, Access Codes, and passwords. Recommended by [PP2600.2] 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-faxforward	X		The TOE allows the administrator to allow or disallow use of the Fax Forward and Fax Archive features.

Table 10: SFR mappings of non-PP2600.2 SFRs and the ST (in the ST, but not required by or hierarchical to SFRs in PP2600.2)

2.1.2 SFR Package for Hardcopy Device Copy Functions ([PP2600.2-CPY])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-CPY] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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).

Table 11: SFR mappings between 2600.2-CPY and the ST

2.1.3 SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions ([PP2600.2-DSR])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-DSR] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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).

Table 12: SFR mappings between 2600.2-DSR and the ST

2.1.4 SFR Package for Hardcopy Device Fax Functions ([PP2600.2-FAX])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-FAX] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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).

Table 13: SFR mappings between 2600.2-FAX and the ST

2.1.5 SFR Package for Hardcopy Device Print Functions ([PP2600.2-PRT])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-PRT] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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).

Table 14: SFR mappings between 2600.2-PRT and the ST

2.1.6 SFR Package for Hardcopy Device Scan Functions ([PP2600.2-SCN])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-SCN] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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).

Table 15: SFR mappings between 2600.2-SCN and the ST

2.1.7 SFR Package for Hardcopy Device Shared-medium Interface Functions ([PP2600.2-SMI])

The following table shows how the SFRs in this SFR package map to the SFRs in the Security Target.

[PP2600.2-SMI] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
FAU_GEN.1	FAU_GEN.1			The ST's FAU_GEN.1 combines the contents of FAU_GEN.1 from the common [PP2600.2] and FAU_GEN.1 from the [PP2600.2] SMI SFR package.
FPT_FDI_EXP.1	FPT_FDI_EXP.1			n/a
FTP_ITC.1	FTP_ITC.1			[CCEVS-PL20] modifies FTP_ITC.1.3.

Table 16: SFR mappings between 2600.2-SMI and the ST

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 Threat Environment

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 low 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

T.DOC.DIS

User Document Data may be disclosed to unauthorized persons.

T.DOC.ALT

User Document Data may be altered by unauthorized persons.

T.FUNC.ALT

User Function Data may be altered by unauthorized persons.

T.PROT.ALT

TSF Protected Data may be altered by unauthorized persons.

T.CONF.DIS

TSF Confidential Data may be disclosed to unauthorized persons.

T.CONF.ALT

TSF Confidential Data may be altered by unauthorized persons.

3.3 Assumptions

3.3.1 Environment of use of the TOE

3.3.1.1 Physical

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.

A.ADMIN.PC.SECURE

The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it.

A.USER.PC.POLICY

User computers are configured and used in conformance with the organization's security policies.

3.3.1.2 Personnel

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.

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.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

3.3.1.3 Connectivity

A.DNS.RELIABLE

When the TOE resolves network hostnames to addresses with the Domain Name System, the Domain Name System provides reliable network addresses.

A.NTP.RELIABLE

When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol provides a reliable time synchronization source for the TOE.

A.SERVICES.RELIABLE

When the TOE uses any of the network services Kerberos, LDAP, SMTP, or syslog, these services provide reliable information and responses to the TOE.

A.WINS.RELIABLE

When the TOE resolves network hostnames to addresses with the Windows Internet Name Service, the Windows Internet Name Service provides reliable network addresses.

3.4 Organizational Security Policies

3.4.1 Included in the PP2600.2 protection profile

P.USER.AUTHORIZATION

To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION

To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

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.

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.

3.4.2 In addition to the PP2600.2 protection profile

P.PJL.PASSWORD

To protect access to documents and resources controlled by the TOE, the PJL Password will be set to a value specified by 9 or more digits.

P.ADMIN.PASSWORD

To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that it is required to perform security-relevant actions through EWS (HTTP) or at the Control Panel.

4 Security Objectives

4.1 Objectives for the TOE

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.

O.CONF.NO_ALT

The TOE shall protect TSF Confidential Data from unauthorized alteration.

O.CONF.NO_DIS

The TOE shall protect TSF Confidential Data from unauthorized disclosure.

O.DOC.NO_ALT

The TOE shall protect User Document Data from unauthorized alteration.

O.DOC.NO_DIS

The TOE shall protect User Document Data from unauthorized disclosure.

O.FUNC.NO_ALT

The TOE shall protect User Function Data from unauthorized alteration.

O.INTERFACE.MANAGED

The TOE shall manage the operation of external interfaces in accordance with security policies.

O.PROT.NO_ALT

The TOE shall protect TSF Protected Data from unauthorized alteration.

O.SOFTWARE.VERIFIED

The TOE shall provide procedures to self-verify executable code in the TSF.

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.

4.2 Objectives for the Operational Environment

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.

OE.ADMIN.PC.SECURE

The TOE Owner shall locate the administrative computer in a physically secured and managed environment and allow only authorized personnel access to it.

OE.USER.PC.POLICY

The TOE Owner shall create a set of security policies to which user computers will conform.

OE.ADMIN.TRUSTED

The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.

OE.AUDIT.REVIEWED

The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

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 to detect potential security violations, and only by authorized 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.

OE.INTERFACE.MANAGED

The IT environment shall provide protection from unmanaged access to TOE external interfaces.

OE.PHYSICAL.MANAGED

The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.

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.

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.

OE.DNS.RELIABLE

When the TOE uses the Domain Name System to resolve hostnames to network addresses, the Domain Name System shall provide a reliable address for the TOE.

OE.NTP.RELIABLE

When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol shall provide a reliable time synchronization source for the TOE.

OE.SERVICES.RELIABLE

When the TOE is configured to use the networks services Kerberos, LDAP, SMTP, or syslog, these services shall provide reliable information and responses to the TOE.

OE.WINS.RELIABLE

When the TOE uses the Windows Internet Name Service to resolve hostnames to network addresses, the Windows Internet Name Service shall provide a reliable address for the TOE.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.AUDIT.LOGGED	P.AUDIT.LOGGING
O.CONF.NO_ALT	T.CONF.ALT
O.CONF.NO_DIS	T.CONF.DIS
O.DOC.NO_ALT	T.DOC.ALT
O.DOC.NO_DIS	T.DOC.DIS
O.FUNC.NO_ALT	T.FUNC.ALT
O.INTERFACE.MANAGED	P.INTERFACE.MANAGEMENT
O.PROT.NO_ALT	T.PROT.ALT
O.SOFTWARE.VERIFIED	P.SOFTWARE.VERIFICATION
O.USER.AUTHORIZED	T.DOC.DIS T.DOC.ALT T.FUNC.ALT T.PROT.ALT T.CONF.DIS T.CONF.ALT P.USER.AUTHORIZATION

Table 17: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.ADMIN.TRAINED	A.ADMIN.TRAINING P.PJL.PASSWORD P.ADMIN.PASSWORD
OE.ADMIN.PC.SECURE	A.ADMIN.PC.SECURE
OE.USER.PC.POLICY	A.USER.PC.POLICY
OE.ADMIN.TRUSTED	A.ADMIN.TRUST
OE.AUDIT.REVIEWED	P.AUDIT.LOGGING
OE.AUDIT_ACCESS.AUTHORIZED	P.AUDIT.LOGGING
OE.AUDIT_STORAGE.PROTECTED	P.AUDIT.LOGGING
OE.INTERFACE.MANAGED	P.INTERFACE.MANAGEMENT
OE.PHYSICAL.MANAGED	A.ACCESS.MANAGED
OE.USER.AUTHORIZED	T.DOC.DIS T.DOC.ALT T.FUNC.ALT T.PROT.ALT T.CONF.DIS T.CONF.ALT P.USER.AUTHORIZATION
OE.USER.TRAINED	A.USER.TRAINING
OE.DNS.RELIABLE	A.DNS.RELIABLE
OE.NTP.RELIABLE	A.NTP.RELIABLE
OE.SERVICES.RELIABLE	A.SERVICES.RELIABLE
OE.WINS.RELIABLE	A.WINS.RELIABLE

Table 18: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.DOC.DIS	The threat: ● User Document Data may be disclosed to unauthorized persons. is countered by: ● O.DOC.NO_DIS which protects D.DOC from unauthorized disclosure. ● O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. ● OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	The threat: ● User Document Data may be altered by unauthorized persons. is countered by: ● O.DOC.NO_ALT which protects D.DOC from unauthorized alteration. ● O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. ● OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	The threat: ● User Function Data may be altered by unauthorized persons. is countered by: ● O.FUNC.NO_ALT which protects D.FUNC from unauthorized alteration. ● O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. ● OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	The threat: ● TSF Protected Data may be altered by unauthorized persons. is countered by: ● O.PROT.NO_ALT which protects D.PROT from unauthorized alteration. ● O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. ● OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	The threat: ● TSF Confidential Data may be disclosed to unauthorized persons. is countered by: ● O.CONF.NO_DIS which protects D.CONF from unauthorized disclosure.

Threat	Rationale for security objectives
	• O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. • OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.ALT	The threat: • TSF Confidential Data may be altered by unauthorized persons. is countered by: • O.CONF.NO_ALT which protects D.CONF from unauthorized alteration. • O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization. • OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.

Table 19: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.ACCESS.MANAGED	The assumption: • 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. is upheld by: • OE.PHYSICAL.MANAGED which establishes a protected physical environment for the TOE.
A.ADMIN.PC.SECURE	The assumption: • The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it. is upheld by: • OE.ADMIN.PC.SECURE which establishes the responsibility of the TOE owner to locate the administrative computer in a physically secured and managed environment and allow only authorized personnel access.
A.USER.PC.POLICY	The assumption:

Assumption	Rationale for security objectives
	• User computers are configured and used in conformance with the organization's security policies. is upheld by: • OE.USER.PC.POLICY which establishes the responsibility of the TOE owner to create a set of security policies to which user computers will conform.
A.USER.TRAINING	The assumption: • TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures. is upheld by: • OE.USER.TRAINED which establishes responsibility of the TOE Owner to provide appropriate User training.
A.ADMIN.TRAINING	The assumption: • 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. is upheld by: • OE.ADMIN.TRAINED which establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	The assumption: • Administrators do not use their privileged access rights for malicious purposes. is upheld by: • OE.ADMIN.TRUST which establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.DNS.RELIABLE	The assumption: • When the TOE resolves network hostnames to addresses with the Domain Name System, the Domain Name System provides reliable network addresses. is upheld by: • OE.DNS.RELIABLE which, when the TOE uses the Domain Name System to resolve hostnames to network addresses, establishes that the Domain Name System shall provide a reliable address for the TOE.
A.NTP.RELIABLE	The assumption: • When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol provides a reliable time synchronization source for the TOE.

Assumption	Rationale for security objectives
	is upheld by: • OE.NTP.RELIABLE which, when the TOE is configured to use the Network Time Protocol as a time synchronization source, establishes that the Network Time Protocol shall provide a reliable time synchronization source for the TOE.
A.SERVICES.RELIABLE	The assumption: • When the TOE uses any of the network services Kerberos, LDAP, SMTP, or syslog, these services provide reliable information and responses to the TOE. is upheld by: • OE.SERVICES.RELIABLE which, when the TOE uses the network services Kerberos, LDAP, SMTP, and syslog, establishes that these services provide reliable information and responses to the TOE.
A.WINS.RELIABLE	The assumption: • When the TOE resolves network hostnames to addresses with the Windows Internet Name Service, the Windows Internet Name Service provides reliable network addresses. is upheld by: • OE.WINS.RELIABLE which, when the TOE uses the Windows Internet Name Service to resolve hostnames to network addresses, establishes that the Windows Internet Name Service shall provide a reliable address for the TOE.

Table 20: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

OSP	Rationale for security objectives
P.USER.AUTHORIZATION	The OSP: • To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner. is enforced by: • O.USER.AUTHORIZED which establishes user identification and authentication as the basis for authorization to use the TOE. • OE.USER.AUTHORIZED which establishes responsibility of the TOE Owner to appropriately grant authorization.
P.SOFTWARE.VERIFICATION	The OSP: • To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

OSP	Rationale for security objectives
	is enforced by: • O.SOFTWARE.VERIFIED which provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	The OSP: • 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. is enforced by: • O.AUDIT.LOGGED which creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration. • OE.AUDIT_STORAGE.PROTECTED which protects exported audit records from unauthorized access, deletion and modifications. • OE.AUDIT_ACCESS.AUTHORIZED which establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records. • OE.AUDIT.REVIEWED which establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	The OSP: • 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. is enforced by: • O.INTERFACE.MANAGED which manages the operation of external interfaces in accordance with security policies. • OE.INTERFACE.MANAGED which establishes a protected environment for TOE external interfaces.
P.PJL.PASSWORD	The OSP: • To protect access to documents and resources controlled by the TOE, the PJL Password will be set to a value specified by 9 or more digits. is enforced by: • OE.ADMIN.TRAINED which establishes responsibility of the TOE Owner to provide appropriate Administrator training. • OE.USER.TRAINED which establishes responsibility of the TOE Owner to provide appropriate User training.
P.ADMIN.PASSWORD	The OSP: • To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that it is required to perform security-relevant actions through EWS (HTTP) or at the Control Panel.

OSP	Rationale for security objectives
	is enforced by: • OE.ADMIN.TRAINED which establishes responsibility of the TOE Owner to provide appropriate Administrator training.

Table 21: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

[PP2600.2-SMI] defines the following extended component:

- FPT_FDI_EXP.1: Restricted forwarding of data to external interfaces

5.1 Class FPT: Protection of the TSF

This section describes the functional requirements for the restrictions of forwarding of data to external interfaces. This extended component is defined in [PP2600.2-SMI].

5.1.1 Restricted forwarding of data to external interfaces (FDI)

Family behaviour

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component levelling

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

There are no management activities foreseen.

Audit: FPT_FDI_EXP.1

There are no audit events foreseen.

5.1.1.1 FPT_FDI_EXP.1 - Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FDI_EXP.1.1 **The TSF shall provide the capability to restrict data received on [assignment:** *list of external interfaces*] **from being forwarded without further processing by the TSF to [assignment:** *list of external interfaces*]**.**

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		PP2600.2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		PP2600.2	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1-ipsec-aes Cryptographic key generation	FCS_CKM.1	CC Part 2	Yes	No	Yes	No
	FCS_CKM.1-ipsec-hmacsha1 Cryptographic key generation	FCS_CKM.1	CC Part 2	Yes	No	Yes	No
	FCS_CKM.2-ipsec-ikev1 Cryptographic key distribution	FCS_CKM.2	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.2-ipsec-ikev2 Cryptographic key distribution	FCS_CKM.2	CC Part 2	Yes	Yes	Yes	No
	FCS_COP.1-job-aes Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1-ipsec-aes Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1-ipsec-rsa Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1-ipsec-hmacsha1 Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
FDP - User data protection	FDP_ACC.1-cac Common access control SFP	FDP_ACC.1	PP2600.2	Yes	No	Yes	No
	FDP_ACC.1-tfac TOE function access control SFP	FDP_ACC.1	PP2600.2	Yes	No	Yes	No
	FDP_ACF.1-cac Common access control functions	FDP_ACF.1	PP2600.2	Yes	No	Yes	No
	FDP_ACF.1-tfac TOE function access control functions	FDP_ACF.1	PP2600.2	Yes	No	Yes	No
	FDP_ITC.1 Import from outside of the TOE		CC Part 2	No	Yes	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FDP_RIP.1 Subset residual information protection		PP2600.2	No	No	Yes	Yes
FIA - Identification and authentication	FIA_ATD.1 Local user attribute definition		PP2600.2	No	No	Yes	No
	FIA_SOS.1 Verification of secrets		CC Part 2	No	No	Yes	No
	FIA_UAU.1 Timing of Control Panel authentication		PP2600.2	No	Yes	Yes	No
	FIA_UAU.2 IPsec authentication before any action		PP2600.2	No	Yes	No	No
	FIA_UAU.7 Control Panel protected authentication feedback		CC Part 2	No	Yes	Yes	No
	FIA_UID.1 Timing of Control Panel identification		PP2600.2	No	Yes	Yes	No
	FIA_UID.2 IPsec identification before any action		PP2600.2	No	Yes	No	No
	FIA_USB.1 User-subject binding		PP2600.2	No	Yes	Yes	No
FMT - Security management	FMT_MOF.1-auth Management of authentication security functions behavior	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MOF.1-faxforward Management of Fax Forward and Fax Archive security functions behavior	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1-perm Management of Permission Set security attributes	FMT_MSA.1	PP2600.2	Yes	No	Yes	Yes
	FMT_MSA.1-pjl Management of PJL Password-based security attributes	FMT_MSA.1	PP2600.2	Yes	No	Yes	Yes
	FMT_MSA.1-tfac Management of TOE function security attributes	FMT_MSA.1	PP2600.2	Yes	No	Yes	Yes
	FMT_MTD.1-auth Management of TSF data	FMT_MTD.1	PP2600.2	Yes	No	Yes	Yes
	FMT_MTD.1-users Management of TSF data	FMT_MTD.1	PP2600.2	Yes	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		PP2600.2	No	No	Yes	No
	FMT_SMR.1 Security roles		PP2600.2	No	No	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FPT - Protection of the TSF	FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces		PP2600.2-SMI	No	No	Yes	No
	FPT_STM.1 Reliable time stamps		PP2600.2	No	No	No	No
	FPT_TST.1 TSF testing		PP2600.2	No	No	Yes	Yes
FTA - TOE access	FTA_SSL.3 Control Panel TSF-initiated termination		PP2600.2	No	Yes	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		PP2600.2-SMI	No	Yes	Yes	Yes

Table 22: Security functional requirements for the TOE

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:

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

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

c) **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 23; none**.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 23: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required); none**.

Auditable event	Relevant SFR(s)	Audit level	Additional information	[PP2600.2] section
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1, FIA_UAU.2	Basic	None required	Common
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1, FIA_UID.2	Basic	Attempted user identity, if available	Common
Use of the management functions	FMT_SMF.1	Minimum	None required	Common
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required	Common

Auditable event	Relevant SFR(s)	Audit level	Additional information	[PP2600.2] section
Changes to the time	FPT_STM.1	Minimum	None required	Common
Termination of an interactive session by the session termination mechanism	FTA_SSL.3	Minimum	None required	n/a
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required	SMI

Table 23: Auditable events

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.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1-ipsec-aes)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **QuickSec AES key generation** and specified cryptographic key sizes **128 bits, 192 bits, 256 bits** that meet the following:

- **[RFC4301] Security Architecture for the Internet Protocol.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment. Key generation is implemented with the ssh random number generator described in section 29.5.3 (pages 1044-1045) of* [QuickSec51]*.*

6.1.2.2 Cryptographic key generation (FCS_CKM.1-ipsec-hmacsha1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **QuickSec HMAC key generation** and specified cryptographic key sizes **96 bits, 160 bits** that meet the following:

- **[RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH**
- **[RFC4301] Security Architecture for the Internet Protocol**
- **[RFC4894] Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment. Key generation is implemented with the ssh random number generator described in section 29.5.3 (pages 1044-1045) of* [QuickSec51]*.*

6.1.2.3 Cryptographic key distribution (FCS_CKM.2-ipsec-ikev1)

FCS_CKM.2.1 The TSF shall distribute *symmetric* cryptographic keys in accordance with a specified cryptographic key distribution method **IKEv1** that meets the following:

- **[RFC2409]The Internet Key Exchange (IKE).**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment.*

6.1.2.4 Cryptographic key distribution (FCS_CKM.2-ipsec-ikev2)

FCS_CKM.2.1 The TSF shall distribute *symmetric* cryptographic keys in accordance with a specified cryptographic key distribution method **IKEv2** that meets the following:

- **[RFC4306] Diffie-Hellman key agreement method defined for the IKEv2 protocol**
- **[RFC4718] IKEv2 Clarifications and Implementation Guidelines.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment.*

6.1.2.5 Cryptographic operation (FCS_COP.1-job-aes)

FCS_COP.1.1 The TSF shall perform **symmetric decryption** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **256 bits** that meet the following:

- **[FIPS197] Advanced Encryption Standard**
- **[SP800-38A]Recommendation for Block Cipher Modes of Operation: Methods and Techniques.**

6.1.2.6 Cryptographic operation (FCS_COP.1-ipsec-aes)

FCS_COP.1.1 The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128 bits, 192 bits, 256 bits** that meet the following:

- **[FIPS197] Advanced Encryption Standard**
- **[SP800-38A]Recommendation for Block Cipher Modes of Operation: Methods and Techniques.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment.*

6.1.2.7 Cryptographic operation (FCS_COP.1-ipsec-rsa)

FCS_COP.1.1 The TSF shall perform **asymmetric decryption for digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits, 2048 bits, 4096 bits** that meet the following:

- **[PKCS1v1.5]Public-Key Cryptography Standard (PKCS) #1: RSA Encryption Standard.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment.*

6.1.2.8 Cryptographic operation (FCS_COP.1-ipsec-hmacsha1)

FCS_COP.1.1 The TSF shall perform **keyed message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA1** and cryptographic key sizes **96 bits** that meet the following:

- **[RFC2104] HMAC: Keyed-Hashing for Message Authentication.**

Application Note: *This algorithm is not implemented by the TOE itself, but by the QuickSec cryptographic library, part of the Operational Environment.*

6.1.3 User data protection (FDP)

6.1.3.1 Common access control SFP (FDP_ACC.1-cac)

FDP_ACC.1.1 The TSF shall enforce the **Common Access Control SFP in Table 24** on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 24**.

Object	Operation(s)	Subject	Access control rules	[PP2600.2] section
D.FUNC	Modify, Delete	U.NORMAL	For stored copy and print jobs in Job Storage with the Job PIN attribute set: From the Control Panel, subjects must be the job owner or know the Job PIN or have the appropriate non-fax Job Storage permission in their Permission Set to delete the job; otherwise, delete access is denied. D.FUNC for Stored Jobs cannot be modified by any user, including U.ADMINISTRATOR. For encrypted stored print jobs: From the Control Panel, subjects must know the job's Job Encryption Password or have the appropriate non-fax Job Storage permission in their Permission Set to delete D.FUNC; otherwise, delete access is denied. For Receive Fax jobs: Subjects must have the appropriate permission in their Permission Set to delete D.FUNC; otherwise, delete access is denied. Modify access is denied to all subjects. For Fax Polling Receive jobs: The subject performing the polling fax function can delete the received object's D.FUNC (i.e., the TOE automatically deletes the job at the end of the function); otherwise, delete access is denied. Modify access is denied to all subjects.	Common

Object	Operation(s)	Subject	Access control rules	[PP2600.2] section
D.DOC	Delete	U.NORMAL	For stored copy and print jobs in Job Storage with the Job PIN attribute set: From the Control Panel, subjects must be the job owner or know the Job PIN or have the appropriate non-fax Job Storage permission in their Permission Set to delete the job; otherwise, delete access is denied. For encrypted stored print jobs: From the Control Panel, subjects must know the job's Job Encryption Password or have the appropriate non-fax Job Storage permission in their Permission Set to delete D.DOC; otherwise, delete access is denied. For Receive Fax jobs: From the Control Panel, subjects must have the appropriate permission in their Permission Set to delete the objects; otherwise, delete access is denied. By default, U.NORMAL users do not have the appropriate permission. (Network access is not possible.) For Fax Polling Receive jobs: The subject performing the outbound fax polling function can delete the job (i.e., the TOE automatically deletes the job at the end of the function); otherwise, delete access is denied.	Common
D.DOC+DSR D.DOC+SCN	Read	U.NORMAL	Scan jobs are not stored in Job Storage while the scan is in progress, but in temporary storage not accessible to any other user. The user scanning the document specifies its disposition (e.g., network folder, email, job storage) at the time of the scan and the scan job becomes the job type appropriate for the requested disposition upon completion of the scan. For stored copy jobs in Job Storage with the Job PIN attribute set: Subjects must be the job owner or know the Job PIN to read the object; otherwise, read access is denied.	DSR, SCN
D.DOC+DSR D.DOC+PRT	Read	U.NORMAL	For print jobs in Job Storage with the Job PIN attribute set: Subjects must be the job owner or know the Job PIN to read the object; otherwise, read access is denied. For encrypted stored print jobs: Subjects must know the job's Job Encryption Password to read the object, otherwise, read access is denied.	DSR, PRT

Object	Operation(s)	Subject	Access control rules	[PP2600.2] section
D.DOC+DSR D.DOC+FAXIN D.DOC+FAXOUT	Read	U.NORMAL	(D.DOC+FAXIN+DSR) For Receive Fax jobs: Subjects must have the appropriate permission in their Permission Set to read the objects; otherwise, read access is denied. (D.DOC+FAXIN) For Fax Polling Receive jobs: The subject performing the outbound fax polling function can read the object; otherwise, read access is denied. (D.DOC+FAXOUT) Send Fax jobs cannot be read by any subject.	DSR, FAX
D.DOC+CPY	Read, Modify	U.NORMAL	There are no access control restrictions for read and modify access.	CPY

Table 24: Common Access Control SFP

6.1.3.2 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.**

6.1.3.3 Common access control functions (FDP_ACF.1-cac)

FDP_ACF.1.1 The TSF shall enforce the **Common Access Control SFP in Table 24** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 24, and for each, the indicated security attributes in Table 24.**

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 24 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:

a) U.ADMINISTRATOR can delete any D.DOC without providing a Job PIN or job encryption password.

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

6.1.3.4 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:**

a) Users: Control Panel users;

Functions: F.CPY, F.DSR, F.FAX, F.PRT, F.SCN, F.SMI;
Security attributes: User Role as defined by the user's Permission Set, authentication database function association

b) Users: Network Client Computers, Administrative Computer;
Functions: F.DSR, F.PRT, F.SMI;
Security attributes: User Role as defined by the IP address, X.509v3 certificate.

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

a) the user is explicitly authorized by U.ADMINISTRATOR to use a function

b) a Network Client Computer 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**.

6.1.3.5 Import from outside of the TOE (FDP_ITC.1)

FDP_ITC.1.1 The TSF shall enforce the **TOE Function Access Control SFP** when importing *cryptographic certificates* ~~user data~~, controlled under the SFP, from outside the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the *cryptographic certificates* ~~user data~~ when imported from outside of the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing *cryptographic certificates* ~~user data~~ controlled under the SFP from outside the TOE: **none**.

Application Note: *Identity and CA certificates become TSF data when imported.*

6.1.3.6 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**.

6.1.4 Identification and authentication (FIA)

6.1.4.1 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:

a) Control Panel users:

1. User Role (defined by Permission Set)

2. Access Code (Local Device Sign In only)

b) IPsec users:

1. User Role (defined by IP address)

6.1.4.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the requirement:**

a) Job PINs shall be 4 digits.

6.1.4.3 Timing of Control Panel authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **viewing of the Control Panel help screens and selection of an authentication mechanism** on behalf of the *Control Panel* user to be performed before the user is authenticated.

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.

6.1.4.4 IPsec authentication before any action (FIA_UAU.2)

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~~.

6.1.4.5 Control Panel protected authentication feedback (FIA_UAU.7)

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

6.1.4.6 Timing of Control Panel identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow **viewing of the Control Panel help screens and selection of an authentication mechanism** on behalf of the *Control Panel* user to be performed before the user is identified.

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.

6.1.4.7 IPsec identification before any action (FIA_UID.2)

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~~.

6.1.4.8 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 and User Identifier**.

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 subjects acting on 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**.

6.1.5 Security management (FMT)

6.1.5.1 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 behaviour of** the functions **authentication** to **U.ADMINISTRATOR**.

6.1.5.2 Management of Fax Forward and Fax Archive security functions behavior (FMT_MOF.1-faxforward)

FMT_MOF.1.1 The TSF shall restrict the ability to **disable, enable** the functions **Fax Forwarding, Fax Archive** to **U.ADMINISTRATOR**.

6.1.5.3 Management of Permission Set security attributes (FMT_MSA.1-perm)

FMT_MSA.1.1 The TSF shall enforce the **Common Access Control SFP in Table 24 and TOE Function Access Control SFP** to restrict the ability to **modify, create, associate with a user or group** the security attributes **Permission Set** to **U.ADMINISTRATOR**.

6.1.5.4 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 24** to restrict the ability to **modify, set** the security attributes **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 must not be deleted in the evaluated configuration.*

6.1.5.5 Management of TOE function security attributes (FMT_MSA.1-tfac)

FMT_MSA.1.1 The TSF shall enforce the **TOE Function Access Control SFP** to restrict the ability to **perform the following operations on** the security attributes

- **User Role as defined by the IP address: add, delete operations**
- **X.509v3 certificate: add, modify, delete operations**
- **authentication database function association: modify operation**

to **U.ADMINISTRATOR**.

6.1.5.6 Management of TSF data (FMT_MTD.1-auth)

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

a) X.509v3 certificates: add, delete operations

b) Allowed IP addresses for Network Client, Administrative, and Server computers: add, delete

to **U.ADMINISTRATOR**.

6.1.5.7 Management of TSF data (FMT_MTD.1-users)

FMT_MTD.1.1 The TSF shall restrict the ability to **modify, initialize** the **Device User Accounts** to **U.ADMINISTRATOR**.

6.1.5.8 Specification of management functions (FMT_SMF.1)

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

a) Authentication database selection management

b) Local Device authentication data (Access Code) management

c) Fax forwarding and fax archive management

d) Permission Set management

e) PJL Password management

f) X.509v3 Certificate management

g) IP address management for Network Client Computers, the Administrative Computer, and Server Computers.

6.1.5.9 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, U.SERVER.AUTHD** .

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 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**.

6.1.6.2 Reliable time stamps (FPT_STM.1)

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

6.1.6.3 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

a) PJL Password - PJL Password verification

b) System Clock - timestamp verification

c) Local Device Sign In - user Access Code verification

d) LDAP Sign In - LDAP settings verification

e) Windows Sign In (via Kerberos) - Windows Settings verification.

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

a) PJL Password

b) Local Device authentication database

c) Device Administrator Password

d) User and administrator authentication configuration data (including Permission Sets and sign-in method assigned to top-level Control Panel application).

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

6.1.7 TOE access (FTA)

6.1.7.1 Control Panel TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate ~~an~~ *a Control Panel* interactive session after ~~a~~ *any one of:*

a) the user starts any job (if configured by U.ADMINISTRATOR)

b) a period of time, configurable by U.ADMINISTRATOR, of user inactivity.

6.1.8 Trusted path/channels (FTP)

6.1.8.1 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 ~~channel~~*communicated* 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 Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.AUDIT.LOGGED

Security Functional Requirements	Objectives
FAU_GEN.2	O.AUDIT.LOGGED
FCS_CKM.1-ipsec-aes	O.CONF.NO_DIS, O.DOC.NO_DIS
FCS_CKM.1-ipsec-hmacsha1	O.CONF.NO_ALT, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT
FCS_CKM.2-ipsec-ikev1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FCS_CKM.2-ipsec-ikev2	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FCS_COP.1-job-aes	O.DOC.NO_ALT, O.DOC.NO_DIS
FCS_COP.1-ipsec-aes	O.CONF.NO_DIS, O.DOC.NO_DIS
FCS_COP.1-ipsec-rsa	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FCS_COP.1-ipsec-hmacsha1	O.CONF.NO_ALT, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT
FDP_ACC.1-cac	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT
FDP_ACC.1-tfac	O.USER.AUTHORIZED
FDP_ACF.1-cac	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT
FDP_ACF.1-tfac	O.USER.AUTHORIZED

Security Functional Requirements	Objectives
FDP_ITC.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FDP_RIP.1	O.DOC.NO_DIS
FIA_ATD.1	O.USER.AUTHORIZED
FIA_SOS.1	O.USER.AUTHORIZED
FIA_UAU.1	O.INTERFACE.MANAGED, O.USER.AUTHORIZED
FIA_UAU.2	O.INTERFACE.MANAGED, O.USER.AUTHORIZED
FIA_UAU.7	O.CONF.NO_DIS
FIA_UID.1	O.AUDIT.LOGGED, O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.INTERFACE.MANAGED, O.PROT.NO_ALT, O.USER.AUTHORIZED
FIA_UID.2	O.AUDIT.LOGGED, O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.INTERFACE.MANAGED, O.PROT.NO_ALT, O.USER.AUTHORIZED
FIA_USB.1	O.USER.AUTHORIZED
FMT_MOF.1-auth	O.PROT.NO_ALT
FMT_MOF.1-faxforward	O.INTERFACE.MANAGED
FMT_MSA.1-perm	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.USER.AUTHORIZED
FMT_MSA.1-pjl	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT

Security Functional Requirements	Objectives
FMT_MSA.1-tfac	O.USER.AUTHORIZED
FMT_MTD.1-auth	O.CONF.NO_ALT, O.CONF.NO_DIS, O.PROT.NO_ALT
FMT_MTD.1-users	O.CONF.NO_ALT, O.CONF.NO_DIS, O.PROT.NO_ALT
FMT_SMF.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FMT_SMR.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.USER.AUTHORIZED
FPT_FDI_EXP.1	O.INTERFACE.MANAGED
FPT_STM.1	O.AUDIT.LOGGED
FPT_TST.1	O.SOFTWARE.VERIFIED
FTA_SSL.3	O.INTERFACE.MANAGED, O.USER.AUTHORIZED
FTP_ITC.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT

Table 25: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.AUDIT.LOGGED	The objective:

Security objectives	Rationale
	• 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. • FIA_UID.1 and FIA_UID.2 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: • The TOE shall protect TSF Confidential Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec-hmacsha1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC-SHA1 in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • FCS_COP.1-ipsec-hmacsha1 which specifies an HMAC algorithm used by the TOE in IPsec. • FDP_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MTD.1-auth and 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: • The TOE shall protect TSF Confidential Data from unauthorized disclosure. is met by:

Security objectives	Rationale
	• FCS_CKM.1-ipsec-aes which specifies the type of cryptographic keys generated by the TOE for use with AES in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-ipsec-aes which specifies the AES encryption/decryption algorithms used by the TOE in IPsec. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • FDP_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FIA_UAU.7 which masks the display of certain passwords and PINs during authentication. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MTD.1-auth and 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: • The TOE shall protect User Document Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec-hmacsha1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC-SHA1 in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-job-aes which specifies the AES decryption algorithm used by the TOE to process encrypted jobs. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • FCS_COP.1-ipsec-hmacsha1 which specifies an HMAC algorithm used by the TOE in IPsec. • 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.

Security objectives	Rationale
	• FDP_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm and FMT_MSA.1-pjl which support access control function by enforcing control of security attributes. • 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: • The TOE shall protect User Document Data from unauthorized disclosure. is met by: • FCS_CKM.1-ipsec-aes which specifies the type of cryptographic keys generated by the TOE for use with AES in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-job-aes which specifies the AES decryption algorithm used by the TOE to process encrypted jobs. • FCS_COP.1-ipsec-aes which specifies the AES encryption/decryption algorithms used by the TOE in IPsec. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • 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_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FDP_RIP.1 which enforces protection by making residual data unavailable. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm and FMT_MSA.1-pjl which support access control function by enforcing control of security attributes. • 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.

Security objectives	Rationale
O.FUNC.NO_ALT	The objective: • The TOE shall protect User Function Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec-hmacsha1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC-SHA1 in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • FCS_COP.1-ipsec-hmacsha1 which specifies an HMAC algorithm used by the TOE in IPsec. • 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_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm and FMT_MSA.1-pjl which support access control function by enforcing control of security attributes. • 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: • The TOE shall manage the operation of external interfaces in accordance with security policies. is met by: • FIA_UAU.1 and FIA_UAU.2 which enforce management of external interfaces by requiring user authentication. • FIA_UID.1 and FIA_UID.2 which enforce management of external interfaces by requiring user identification. • FMT_MOF.1-faxforward which allows the administrator to allow or disallow use of the Fax Forward and Fax Archive features. • 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.

Security objectives	Rationale
	• FTA_SSL.3 which enforces management of external interfaces by terminating inactive sessions.
O.PROT.NO_ALT	The objective: • The TOE shall protect TSF Protected Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec-hmacsha1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC-SHA1 in IPsec. • FCS_CKM.2-ipsec-ikev1 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 in IPsec. • FCS_CKM.2-ipsec-ikev2 which specifies the cryptographic key distribution methods used by the TOE in IKEv2 in IPsec. • FCS_COP.1-ipsec-rsa which specifies the RSA decryption algorithms used by the TOE. • FCS_COP.1-ipsec-hmacsha1 which specifies an HMAC algorithm used by the TOE in IPsec. • FDP_ITC.1 which supports control of trusted channels for communication of data over Shared-medium Interfaces. • FIA_UID.1 and FIA_UID.2 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_MTD.1-auth and 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 the TOE include self-tests.
O.USER.AUTHORIZED	The objective: • 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:

Security objectives	Rationale
	• 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_SOS.1 which specifies the password/PIN strength of certain authentication mechanisms. • FIA_UAU.1 and FIA_UAU.2 which enforce authorization by requiring user authentication. • FIA_UID.1 and FIA_UID.2 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-perm and FMT_MSA.1-tfac which support access control function by enforcing control of security attributes. • FMT_SMR.1 which supports authorization by requiring security roles. • FTA_SSL.3 which enforces authorization by terminating inactive sessions.

Table 26: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FCS_CKM.1-ipsec-aes	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2-ipsec-ikev1 FCS_CKM.2-ipsec-ikev2 FCS_COP.1-ipsec-aes
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.

Security Functional Requirement	Dependencies	Resolution
FCS_CKM.1-ipsec-hmacsha1	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2-ipsec-ikev1 FCS_CKM.2-ipsec-ikev2 FCS_COP.1-ipsec-hmacsha1
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FCS_CKM.2-ipsec-ikev1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1-ipsec-aes FCS_CKM.1-ipsec-hmacsha1
	FCS_CKM.4	This dependency is unresolved. The distributed symmetric keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FCS_CKM.2-ipsec-ikev2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1-ipsec-aes FCS_CKM.1-ipsec-hmacsha1
	FCS_CKM.4	This dependency is unresolved. The distributed symmetric keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FCS_COP.1-job-aes	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. The keys used for decryption are created outside the TOE and included as input with the print job.
	FCS_CKM.4	This dependency is unresolved. The keys used for decryption and data authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FCS_COP.1-ipsec-aes	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1-ipsec-aes
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption, decryption, and data authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.

Security Functional Requirement	Dependencies	Resolution
FCS_COP.1-ipsec-rsa	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1 No RSA keys are generated by the TOE in the evaluated configuration. All RSA keys used by the TOE are found in imported certificates.
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption and decryption are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FCS_COP.1-ipsec-hmacsha1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1-ipsec-hmacsha1
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption, decryption, and data authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except in the intended context.
FDP_ACC.1-cac	FDP_ACF.1	FDP_ACF.1-cac
FDP_ACC.1-tfac	FDP_ACF.1	FDP_ACF.1-tfac
FDP_ACF.1-cac	FDP_ACC.1	FDP_ACC.1-cac
	FMT_MSA.3	This dependency is unresolved. The Job PIN, Job Encryption Password, PJL Password, and Permission Sets do not have default values and do not allow for the specification of alternative initial values.
FDP_ACF.1-tfac	FDP_ACC.1	FDP_ACC.1-tfac
	FMT_MSA.3	This dependency is unresolved. The IP address, X.509 certificates, authentication database function association, and Permission Sets do not have default values and do not allow for the specification of alternative initial values.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1-tfac
	FMT_MSA.3	This dependency is unresolved. The IP address, X.509 certificates, authentication database function association, and Permission Sets do not have default values and do not allow for the specification of alternative initial values.

Security Functional Requirement	Dependencies	Resolution
FDP_RIP.1	No dependencies.	
FIA_ATD.1	No dependencies.	
FIA_SOS.1	No dependencies.	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies.	
FIA_UID.2	No dependencies.	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1-auth	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1-faxforward	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1-perm	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1-cac FDP_ACC.1-tfac
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1-pjl	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1-cac
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1-tfac	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1-tfac
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1-auth	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1-users	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	

Security Functional Requirement	Dependencies	Resolution
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FDI_EXP.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FPT_STM.1	No dependencies.	
FPT_TST.1	No dependencies.	
FTA_SSL.3	No dependencies.	
FTP_ITC.1	No dependencies.	

Table 27: TOE SFR dependency analysis

6.2.4 Internal consistency and mutual support of SFRs

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components as specified in [CC] part 3, augmented by ALC_FLR.2.

The following table shows the Security assurance requirements, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No
	ADV_TDS.1 Basic design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3	No	No	No	No
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_FLR.2 Flaw reporting procedures	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 28: Security assurance requirements

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 [PP2600.2]. 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 [PP2600.2].

7 TOE Summary Specification

7.1 TOE Security Functionality

The following section explains how the security functions are implemented by the hardcopy device (HCD). 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 and certificate management
- User and access management

7.1.1 Auditing

The TOE performs auditing of security relevant functions. The TOE connects and sends audit records to a syslog server (part of the Operational Environment) for long-term storage and audit review. The records sent to the syslog server by the TOE are only those generated by the TOE while the syslog server has an established connection with the TOE. If the connection between the TOE and syslog server breaks and is later reestablished, only records generated by the TOE after the connection is reestablished are sent to the syslog server. Both the Jetdirect Inside and HDC System firmware generate audit records.

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 time source used for the audit record timestamps is discussed in section 7.1.4.3.

This section maps to the following SFRs:

- FAU_GEN.1
- FAU_GEN.2

7.1.2 Identification and authentication (I&A)

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

The following interfaces support I&A:

- Control Panel
- IPsec

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

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

7.1.2.1 Control Panel I&A

The Control Panel interface supports both local and remote authentication mechanisms. The following authentication mechanisms are allowed with the evaluated configuration:

- Local authentication mechanism(s):
  - Local Device Sign In
- Remote authentication mechanism(s):
  - LDAP Sign In
  - Windows Sign In (via Kerberos)

(The servers for the remote authentication mechanisms are part of the Operational Environment.)

The Control Panel also allows both non-administrative users (U.NORMAL) and administrative users (U.ADMINISTRATOR) to sign in. Prior to sign in, the Control Panel allows users to select a sign in method, sign in to the TOE, or get help on various printer functions.

Local Device Sign In is only available through the Control Panel. The TOE contains a local user database for defining non-administrative (U.NORMAL, by default) device user accounts used to support the Local Device Sign In mechanism. Each device user account contains the following security attribute:

- Access Code (8 digits)

The Access Code is a number that serves as both the user identifier and the authentication secret. Each user's Access Code is unique from all other Local Device users. In the evaluated configuration, the Access Code length must be 8 digits, which is the largest length for an Access Code allowed by the TOE. The length of the Access Code is manually enforced by the administrator.

The one exception is the Local Device Administrator Access Code, also known as the Device Administrator Password. While stored on the device, this password can be as long as 16 characters and composed of letters, numbers, and special characters. The Device Administrator Password can also be used to sign in to EWS or the Web Services interface from a remote computer in addition to signing in at the Control Panel.

Like Local Device Sign In, the remote authentication mechanisms are only used by the Control Panel. The TOE receives authentication credentials from the Control Panel users and passes the credentials to the remote authentication mechanism. 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.

When a user successfully logs in to the Control Panel, the Permission Set associated with that user is bound to that user instance and defines the user's User Role.

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

This section maps to the following SFRs:

- FIA_ATD.1 (Access Code, User Role)
- FIA_UAU.1
- FIA_UAU.7
- FIA_UID.1
- FIA_USB.1
- FMT_SMR.1

7.1.2.2 IPsec I&A

The TOE uses IPsec to mutually authenticate the following user types:

- Administrative Computer (U.ADMINISTRATOR)
- Network Client Computers (U.NORMAL)
- Authenticated Server Computers (U.SERVER.AUTHD)

IPsec uses X.509v3 certificates via the IKE protocol to authenticate a client computer. Individual client computer certificates are maintained by each client computer, not by the TOE. The TOE uses the client computer's IP address to determine the client computer's User Role. The TOE's internal firewall maintains a list of IP addresses of client computers that can connect to the TOE as a Network Client Computer and as the Administrative Computer. If a client computer has an unrecognized certificate or an IP address that is not defined in the internal firewall as either the Administrative Computer or a Network Client Computer, then the client computer is not allowed to connect to the TOE. The TOE also uses IP addresses and X.509v3 certificates via the IKE protocol to connect to the Authenticated Server Computers.

The TOE supports the following versions of the IKE protocol:

- IKEv1 ([RFC2409] and [RFC4109])
- IKEv2 ([RFC4306] and [RFC4718])

The TOE must use IKE Main Mode for key exchange in the evaluated configuration.

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 do not 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.)

Both the Administrative Computer and the Network Client Computers can access the PJL Interface on port 9100, but only the Administrative Computer can access the EWS (HTTP) interface, Web Services interface (OXPd and SOAP/XML), and SNMP interface.

IP address management is discussed in section 7.1.3.6. Certificate management is discussed in section 7.1.6.

This section maps to the following SFRs:

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1
- FMT_SMR.1

7.1.3 Data protection and access control

7.1.3.1 Permission Sets

For Control Panel users, the TOE uses a user's User Role (as determined by each user's Permission Set) to determine a user's access to many TOE functions. Permission Sets can be created, modified, and associated with users and groups by U.ADMINISTRATOR. By default, the TOE includes the following Permission Sets:

- Device Administrator (U.ADMINISTRATOR)
- Device User (U.NORMAL)

Permissions in a Permission Set include permissions as high-level as copy, print, scan, and fax. They also include more granular permissions that control administrative functions like the ability to print a received incoming fax and the ability to delete any non-fax Job Storage job. Each permission in a Permission Set has two possible values: allowed and disallowed.

This section maps to the following SFRs:

- FMT_MSA.1-perm
- FMT_SMF.1

7.1.3.2 Job PINs

Users can control access to each print and stored copy job that they place on the HCD by assigning a Job PIN to each job. A Job PIN limits access to a print or stored copy job while the job resides on the HCD and allows a user to control when the job is printed so that physical access to the hard copies can be controlled. A Job PIN must be 4 digits (0000-9999) in length. Only one Job PIN is permitted per job.

A Job PIN can only be assigned to a job at job creation time. A user assigns a Job PIN to a stored copy job via the Control Panel. A user assigns a Job PIN to a print job via the client computer. Once a Job PIN is set on a job, it cannot be changed. A job with a Job Encryption Password cannot be assigned a Job PIN.

This section maps to the following SFRs:

- FIA_SOS.1

The Job PIN is initialized by the TOE in some circumstances, but this does not change TOE behavior, therefore no management SFR is required.

7.1.3.3 Job Encryption Passwords

The TOE can store and decrypt encrypted stored print jobs received from a client computer. A stored print job is first encrypted by the client computer using a user-specified Job Encryption Password. The job is then sent encrypted to the TOE and stored encrypted by the TOE. To decrypt the job, a Control Panel user must enter the correct Job Encryption Password used to encrypt the job. Only one Job Encryption Password is permitted per job.

A Job Encryption Password can only be assigned to a job at job creation time. A user assigns a Job Encryption Password to a print job via the client computer. Once a Job Encryption Password is set on a job, it cannot be changed. A job with a Job Encryption Password cannot be assigned a Job PIN.

This section maps to the following SFRs:

- FCS_COP.1-job-aes

7.1.3.4 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 PJL 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 with PJL commands. The administrator must also know the PJL Password in order to modify it.

This section maps to the following SFRs:

- FMT_MSA.1-pjl
- FMT_SMF.1

7.1.3.5 Common access control

The TOE protects each non-fax job in Job Storage from non-administrative users through the use of a user identifier and either a Job PIN or a Job Encryption Password. The user identifier for a print job received from a client computer is either assigned by that client computer or assigned by the user sending the print job from the client computer. For all other types of jobs, the user identifier is assigned by the TOE. Every non-fax job in Job Storage is assigned either a Job PIN or a Job Encryption Password by the user at job creation time. If the TOE receives a non-fax job from a client computer without either a Job PIN or a Job Encryption Password, the TOE cancels the job.

The User Role, as defined by the user's Permission Set, defines each user's access. The default rules for a non-administrative U.NORMAL User Role for accessing a non-fax job in Job Storage are:

- if the job is Job PIN protected:
  - the job owner (i.e., the authenticated user who matches the job's user identifier) can access (read/delete D.DOC) the job without supplying the Job PIN
  - any non-owner authenticated user who supplies the correct Job PIN can access (read/delete D.DOC) the job
- if the job is Job Encryption Password protected, any authenticated user who supplies the correct Job Encryption Password can access (read/delete D.DOC) the job

By default, a Control Panel administrator (U.ADMINISTRATOR) has a permission in their Permission Set that allows them to delete Job Storage jobs.

The TOE protects each fax job in Job Storage through the Permission Set mechanism. A user must have a specific fax permission in their Permission Set to access (read/delete D.DOC) incoming fax jobs stored in Job Storage. By default, only U.ADMINISTRATOR has this permission enabled. Faxes are automatically deleted by the TOE once they are printed.

The Fax Polling Receive function of an HCD allows an authorized user (U.NORMAL) to request a fax from another fax device over the analog fax phone line via the Control Panel. This is called a Fax Polling Receive job (D.DOC+FAXIN). The user must be authenticated via the Control Panel to perform this function. In the evaluated configuration, outbound fax polling requests are allowed.

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 temporary owner of these faxes, the user can read these faxes, and the user deletes these faxes. The user cannot modify these faxes.

Scan jobs are ephemeral and not stored in Job Storage. Only the user performing the scan can access the job on the HCD.

This section maps to the following SFRs:

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

7.1.3.6 TOE function access control

The TOE controls Control Panel access to TOE functions through the use of Permission Sets. When the option to allow alternate sign-in methods is enabled, the TOE can also use these authentication mechanisms to control access. When the option for alternate sign-in methods is enabled, the access a user is given is based only on the permissions associated with User Role (Permission Set) with which they are associated. If the option is disabled, access to certain applications is also based on the sign-in method used.

These mechanisms require TOE users to authenticate themselves in order to perform TOE functions with the exception that users do not need to authenticate to access help screens. The authentication process assigns a User Role to the authenticated user in the form of a Permission Set. Access to each TOE device function is configurable in a Permission Set by an administrator. A user can perform any function permitted in any Permission Set that is associated with a User Role assigned to the user.

In addition, the Control Panel can have different authentication mechanisms assigned to the major TOE functions (e.g., copy, fax) by the administrator. If a function requires LDAP authentication and the user only has a Local Device account, the user will not be able to access that function. Therefore, a Control Panel user can perform the [PP2600.2] functions of F.CPY, F.DSR, F.FAX, F.PRT, F.SCN, and F.SMI as determined by each user's Permission Set.

The TOE distinguishes between Network Client Computers and the Administrative Computer based on each system's IP address. The TOE uses the internal firewall to make this determination. Only an administrator can explicitly authorize a client computer to be a Network Client Computer or Administrative Computer. In addition, Network Client Computers and the Administrative Computer must be authenticated using IPsec and X.509v3 certificates in order to access the functions. The [PP2600.2] functions available to an authorized client computer are F.DSR, F.PRT, and F.SMI.

This section maps to the following SFRs:

- FDP_ACC.1-tfac
- FDP_ACF.1-tfac

7.1.3.7 Residual information protection

When the TOE deletes an object defined in section 6.1.3.6, the contents of the object are no longer available to TOE users.

This section maps to the following SFR:

- FDP_RIP.1

7.1.4 Protection of the TSF

7.1.4.1 Restricted forwarding of data to external interfaces (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 [PP2600.2] and duplicated in section 8.2 of this Security Target. This implies that an administrator can configure the HCD to have a distinct functional separation between the analog fax phone line and the Shared-medium Interface (i.e., network interface) of the TOE. The administrator can disable the fax feature "Fax Archive" to prevent data and commands from being sent from the Public Switched Telephone Network (PSTN) to the local network. The administrator can also disable the Fax Forward feature which receives a fax, then forwards the fax over the phone line to another fax machine.

This section maps to the following SFR:

- FMT_MOF.1-faxforward
- FPT_FDI_EXP.1

7.1.4.2 TSF self-testing

The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of correct operations tests, TSF Data integrity tests, and integrity tests of TSF executable code. The specific security related tests available to the administrator are listed in FPT_TST.1. In some cases, the tests can only be executed if the system is configured to use the feature being tested. For example, the LDAP Settings verification test requires LDAP Sign In to be configured prior to executing the test. The tests that may be available during self-test include:

- PJL Password verification
- Timestamp verification (verify a Network Time Server is configured and responding)
- Device User Access Code verification
- LDAP settings verification
- Windows Setting verification

This section maps to the following SFR:

- FPT_TST.1

7.1.4.3 Reliable timestamps

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

The administrator must configure the device to synchronize the system clock via a Network Time Protocol (NTP) server.

This section maps to the following SFR:

- FPT_STM.1

7.1.5 TOE access protection

The following session termination mechanisms are supported by the TOE:

- Inactivity timeout
- Automatic logout

7.1.5.1 Inactivity timeout

The TOE supports an inactivity timeout for Control Panel sessions. 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 the administrator via EWS (HTTP) or with Web Jetadmin. Only one inactivity period exists per TOE.

This section maps to the following SFR:

- FTA_SSL.3

7.1.5.2 Automatic logout

The administrator can optionally configure the TOE to automatically sign users out after starting a job. The user can be signed out immediately or with a delay of 10 seconds during which time the user can select to remain signed in. If enabled, after initiating a job, the TOE displays a screen informing the user of job termination immediately or in 10 seconds. If given the option and the user chooses to remain signed in, the Inactivity Timeout timer is started.

This section maps to the following SFR:

- FTA_SSL.3

7.1.6 Trusted channel communication and certificate management

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 TOE also ensures the cryptographic operations are validated during policy processing such as validating digital signatures or encrypting and decrypting data. The following table provides a list of the mechanisms used to protect these channels.

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

Secure Protocol	Supported Functions
	• all syslog server connections – these connections are initiated by the TOE

Table 29: Trusted channel connections

The TOE includes IPsec as means to provide trusted channel communications.

IPsec uses X.509v3 certificates, the ESP, ISAKMP, IKEv1, and IKEv2 protocols, and the cryptographic algorithms listed below to protect communications.

The cryptographic functions used by IPsec are implemented in the QuickSec cryptographic library version 5.1 ([QuickSec51]) which is produced by SafeNet, Inc. The QuickSec library is part of the Operational Environment, not the TOE. The TOE prepares the data and invokes the appropriate functions, but code in the QuickSec library performs the processing and calculations required. SafeNet, Inc. performs regular and rigorous developer testing of the implementation of the cryptographic algorithms in the QuickSec library.

In the evaluated configuration, the supported IPsec cryptographic algorithms are:

- AES-128, AES-192, and AES-256 (Operational Environment)
- HMAC-SHA1 (Operational Environment)

IPsec is conformant to the MUST/MUST NOT requirements of the following IETF RFCs:

- [RFC4301] and [RFC4894] for IPsec
- [RFC4303] for ESP
- [RFC4306] for ISAKMP
- [RFC4109] and [RFC4894] for IKEv1
- [RFC4306], [RFC4718], and [RFC4894] for IKEv2.

The TOE can maintain two X.509v3 certificates for IPsec in the Jetdirect certificate store: an Identity certificate and a Certificate Authority (CA) certificate. The Identity certificate cannot be deleted but can be overwritten with another Identity certificate (by U.ADMINISTRATOR). The CA certificate can be deleted by U.ADMINISTRATOR. The Jetdirect Inside firmware can generate a self-signed certificate, however these certificates are not permitted in the evaluated configuration. The administrator is required to replace the self-signed Identity certificate created by the HCD when first powered on with an Identity certificate created outside the TOE and signed by a Certificate Authority. The EWS (HTTP) interface allows administrators to manage (add, delete) X.509v3 certificates used by IPsec.

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

This section maps to the following SFRs:

- FCS_CKM.1-ipsec-aes
- FCS_CKM.1-ipsec-hmacsha1
- FCS_CKM.2-ipsec-ikev1
- FCS_CKM.2-ipsec-ikev2
- FCS_COP.1-ipsec-aes
- FCS_COP.1-ipsec-hmacsha1
- FCS_COP.1-ipsec-rsa

- FDP_ITC.1
- FMT_MOF.1-auth
- FMT_MTD.1-auth
- FMT_SMF.1
- FTP_ITC.1

7.1.7 User and access management

The TOE supports the following roles:

- Administrators (U.ADMINISTRATOR)
- Users (U.NORMAL)
- Authenticated Servers (U.SERVER.AUTHD)

Administrators maintain and configure the TOE and Operational 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 the SMTP gateway and LDAP.

In addition, the TOE performs many security management functions.

Only administrators can configure the list of Network Client Computers and the Administrative Computer that are allowed to connect to the TOE and the list of Authenticated Server Computers to which the TOE will connect. Administrators can add IP addresses to and delete IP addresses from the list of IP addresses in the TOE that define which computers are Network Client Computers, the Administrative Computer, and the Authenticated Server Computers. Administrators can add and delete the X.509v3 certificates used by IPsec for identifying and authenticating these computers. Administrators can also modify the association of authentication databases with TOE functions (for example, the association of the LDAP authentication database with the copy function).

Administrators can initialize and modify Device User Accounts in the Local Device authentication database.

This section maps to the following SFRs:

- FMT_MSA.1-tfac
- FMT_MTD.1-auth
- FMT_MTD.1-users
- FMT_SMF.1
- FMT_SMR.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES
Advanced Encryption Standard

AH
Authentication Header (IPsec)

CBC
Cipher Block Chaining

CIFS
Common Internet File System

CRV
Constrained Random Verification

CTS
Cipher Text Stealing

DNS
Domain Name System

ESP
Encapsulating Security Payload (IPsec)

EWS
Embedded Web Server

FTP
File Transfer Protocol

HCD
Hardcopy Device

HMAC
Hashed Message Authentication Code

HP
Hewlett-Packard

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

IEEE
Institute of Electrical and Electronics Engineers, Inc.

IKE
Internet Key Exchange (IPsec)

IP
Internet Protocol

IPsec
Internet Protocol Security

ISAKMP
Internet Security Association Key Management Protocol (IPsec)

LCD
Liquid Crystal Display

LDAP
Lightweight Directory Access Protocol

MAC
Message Authentication Code

MFP
Multifunction Product

NTP
Network Time Protocol

OXP
Open Extensibility Platform

OXPd
OXP device layer

PIN
Personal Identification Number

PJL
Printer Job Language

PML
Printer Management Language

PRF
Pseudo-random Function

PSTN
Public Switched Telephone Network

SFR
Security Functional Requirement

SHA
Secure Hash Algorithm

SMTP
Simple Mail Transfer Protocol

SNMP
Simple Network Management Protocol

SOAP
Simple Object Access Protocol

TOE
Target of Evaluation

USB
Universal Serial Bus

WINS
Windows Internet Name Service

XML
Extensible Markup Language

8.2 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, Access Code, and/or password for each user of the product.

Device Administrator Password
The password used to restrict access to administrative tasks via EWS and the Control Panel. This password is also required to associate a user with the Administrator role. In product documentation, it may also be referred to as the Local Device Administrator Password, Local Device Administrator Access Code, the Device Password, or the Administrator Password.

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.

8.3 References

CC	**Common Criteria for Information Technology Security Evaluation**	
	Version	3.1R4
	Date	September 2012
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
CCEVS-PL20	**NIAP CCEVS Policy Letter #20**	
	Date	2010-11-15
	Location	http://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-20.pdf

FIPS197 **Advanced Encryption Standard**
Date 2001-11-26
Location http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

PKCS1v1.5 **Public-Key Cryptography Standard (PKCS) #1: RSA Encryption Standard**
Author(s) RSA Laboratories
Version 1.5
Date November 1993

PP2600.2 **IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20)**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-CPY **SFR Package for Hardcopy Device Copy Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-DSR **SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-FAX **SFR Package for Hardcopy Device Fax Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-PRT **SFR Package for Hardcopy Device Print Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-SCN **SFR Package for Hardcopy Device Scan Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

PP2600.2-SMI **SFR Package for Hardcopy Device Shared-medium Interface Functions**
Version 1.0
Date December 2009
Location http://www.niap-ccevs.org/pp/pp_hcd_eal2_v1.0.pdf

QuickSec51 **QuickSec 5.1 Toolkit Reference Manual**
Author(s) SafeNet, Inc.
Version 1.0
Date December 2009

RFC2104 **HMAC: Keyed-Hashing for Message Authentication**
Author(s) H. Krawczyk, M. Bellare, R. Canetti
Date 1997-02-01
Location http://www.ietf.org/rfc/rfc2104.txt

RFC2404 **The Use of HMAC-SHA-1-96 within ESP and AH**
Author(s) C. Madson, R. Glenn
Date 1998-11-01
Location http://www.ietf.org/rfc/rfc2404.txt

RFC2409 **The Internet Key Exchange (IKE)**
Author(s) D. Harkins, D. Carrel
Date 1998-11-01
Location http://www.ietf.org/rfc/rfc2409.txt

RFC4109 **Algorithms for Internet Key Exchange version 1 (IKEv1)**
Author(s) P. Hoffman
Date 2005-05-01
Location http://www.ietf.org/rfc/rfc4109.txt

RFC4301 **Security Architecture for the Internet Protocol**
Author(s) S. Kent, K. Seo
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4301.txt

RFC4303 **IP Encapsulating Security Payload (ESP)**
Author(s) S. Kent
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4303.txt

RFC4306 **Internet Key Exchange (IKEv2) Protocol**
Author(s) C. Kaufman
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4306.txt

RFC4718 **IKEv2 Clarifications and Implementation Guidelines**
Author(s) P. Eronen, P. Hoffman
Date 2006-10-01
Location http://www.ietf.org/rfc/rfc4718.txt

RFC4894 **Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec**
Author(s) P. Hoffman
Date 2007-05-01
Location http://www.ietf.org/rfc/rfc4894.txt

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**
Author(s) Morris Dworkin
Version NIST Special Publication 800-38A 2001 Edition
Date December 2001
Location http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf