HP LaserJet Enterprise MFP M527 Series, Color LaserJet Enterprise MFP M577 Series, and PageWide Enterprise Color MFP 586 Series Firmware with Jetdirect Inside Security Target

Version: **2.0**

Status: **Final**

Last Update: **2016-06-07**

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®
- SharePoint®
- Windows®

The following term is a trademark of INSIDE Secure in the United States, other countries, or both:

- INSIDE Secure®
- QuickSec®

Legal Notices

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	2016-06-07	Gerardo Colunga (HP Inc.), Scott Chapman (atsec)	Final ST version.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	HP LaserJet Enterprise MFP M527 Series, Color LaserJet Enterprise MFP M577 Series, and PageWide Enterprise Color MFP 586 Series Firmware with Jetdirect Inside Security Target
Version:	2.0
Status:	Final
Date:	2016-06-07
Sponsor:	HP Inc.
Developer:	HP Inc.
Certification Body:	CSEC
Certification ID:	CSEC2015012
Keywords:	HP Inc., HP, Color LaserJet, LaserJet, PageWide, Color MFP, M527, M577, 586, hardcopy device, HCD, multifunction printer, MFP, Jetdirect Inside

1.2 TOE Identification

The TOE is the HP LaserJet Enterprise MFP M527 Series, Color LaserJet Enterprise MFP M577 Series, and PageWide Enterprise Color MFP 586 Series Firmware with Jetdirect Inside.

1.3 TOE Type

The TOE type is the internal firmware providing the functionality of a network multifunction printer (MFP).

1.4 TOE Overview

The TOE models are enterprise network MFPs 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).

The TOE contains functions for copying, printing, faxing, scanning, and storing of documents. These hardcopy devices (HCDs), as they are called in [PP2600.2], are self-contained units that include processors, memory, networking, a storage drive, an image scanner, and a print engine. The operating system, web servers, and Control Panel applications (i.e., applications that run internally on the HCD) reside within the firmware of the HCD.

The TOE is the contents of the firmware with the exception of the operating system and the QuickSec cryptographic library (used by IPsec), which are part of the Operational Environment.

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

Product Family	Models	TOE Firmware Version
LaserJet Enterprise MFP M527 Series	MFP M527dn MFP M527f *Flow* MFP M527c *Flow* MFP M527z	System Firmware version: 2307781_551187 Jetdirect Inside version: JSI23700101
Color LaserJet Enterprise MFP M577 Series	MFP M577dn MFP M577f *Flow* MFP M577c *Flow* MFP M577z	System Firmware version: 2307781_551183 Jetdirect Inside version: JSI23700101
PageWide Enterprise Color MFP 586 Series	MFP 586dn MFP 586f *Flow* MFP 586z	System Firmware version: 2307781_551192 Jetdirect Inside version: JSI23700101

Table 1: TOE Reference

Each model provides the following security features:

- Auditing
- Cryptography
- 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 Required and optional non-TOE hardware, software, and firmware

The following *required* firmware components are considered part of the Operational Environment:

- Operating system (included in the firmware)
- QuickSec cryptographic library module (included in the firmware)

The hardware portion of the HP MFP models is considered part of the Operational Environment. The TOE is evaluated on all of the HP MFP models defined in Table 1 and *requires* one of these models in order to run in the evaluated configuration.

The following *required* components are part of the Operational Environment:

- DNS server
- Syslog server
- WINS server
- One administrative client computer network connected to the TOE in the role of an Administrative Computer

The following *optional* components are part of the Operational Environment:

- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- HP Web Jetadmin fleet management tool
- Windows domain controller/Kerberos server
- LDAP server
- Client computers network connected to the TOE in a non-administrative computer role
- Remote file systems:
  - SMB
  - FTP
- Microsoft SharePoint (useful with *flow* models only)
- SMTP gateway
- Web browser

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

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

The evaluated configuration contains a built-in user identification and authentication database (a.k.a. sign in method) used for Local Device Sign In that is part of the TOE. It also supports a Windows domain controller (via Kerberos) for a feature called Windows Sign In and a Lightweight Directory Access Protocol (LDAP) authentication server for a feature called LDAP Sign In to identify and authenticate users. The Windows domain controller and LDAP server are part of the Operational Environment.

The evaluated configuration supports the optional HP Web Jetadmin (WJA) fleet management tool for administering the TOE. (If the HP WJA tool is to be used to administer the TOE, it must be installed on the Administrative Computer.) This tool 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) Web Services, WS* Web Services, and Simple Network Management Protocol (SNMP) to communicate to the TOE. (The HP WJA tool is part of the Operational Environment.) 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.)

The Universal Serial Bus (USB) ports are disabled in the evaluated configuration.

1.5 TOE Description

1.5.1 TOE architecture

As mentioned previously, the TOE is the firmware of an enterprise MFP designed to be shared by many client computers and human users. It performs the functions of printing, copying, scanning, faxing, and storing of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, to an analog telephone 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).

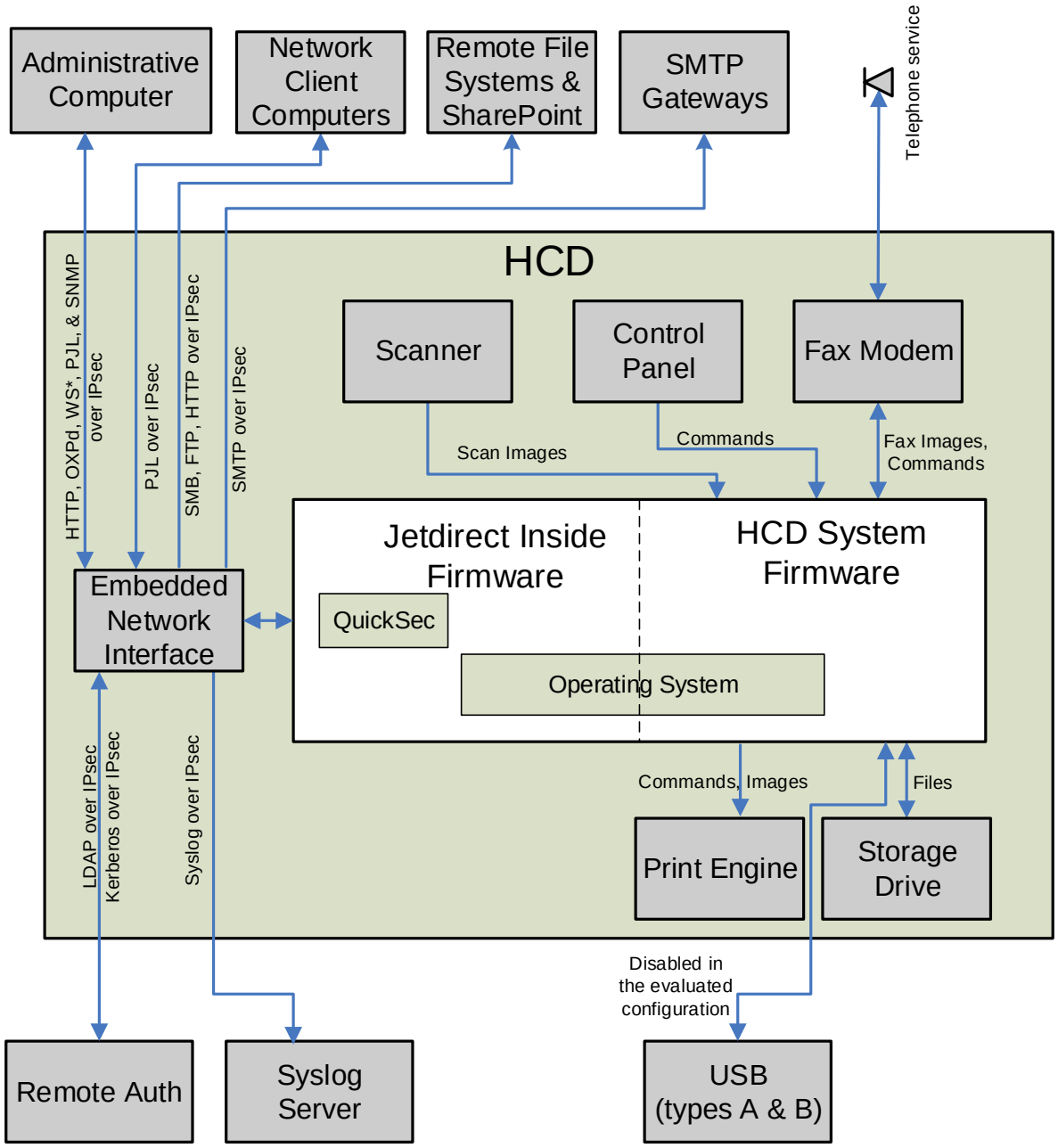

Figure 1: HCD physical diagram

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)
- Simple Network Management Protocol (SNMP)

- Web Services:
    - Open Extensibility Platform device (OXPd) Web Services
    - WS* Web Services

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

The Web Services allow administrators to manage the TOE using HP WJA, which is part of the Operational Environment. The TOE supports both HP's Open Extensibility Platform device (OXPd) Web Services and certain WS* Web Services (conforming to the WS* standards defined by w3.org) accessed via the Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML).

The SNMP network interface allows administrators to remotely manage the TOE using external SNMP-based management tools like HP WJA.

Printer Job Language (PJL) is used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL to send print jobs to the TOE as well as to receive job status. In general, PJL supports password-protected administrative commands, but in the evaluated configuration these commands are disabled. For the purposes of this Security Target, we define the PJL Interface as PJL data sent to port 9100.

The TOE protects all network communications with IPsec, which is part of the embedded Jetdirect Inside firmware. 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 TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) 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 TOE distinguishes between the Administrative Computer and Network Client Computers by using IP addresses, IPsec, and the embedded Jetdirect Inside'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 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 analog fax phone line user can perform is to transmit a fax to the TOE.

Some fax devices can hold a fax until another fax device requests that the fax be sent. Users can use the Fax Polling Receive function of the TOE to retrieve faxes from other fax devices. This is called a Fax Polling Receive job by this document. To perform this function, the user authenticates via the Control Panel and initiates the function by entering the phone number of the other fax device. The TOE will dial the other fax device, negotiate a fax session, and request the other fax device to transfer the held fax to

the TOE via the negotiated fax session. The TOE prints the fax as it receives it. The TOE doesn't not accept fax polling requests from other fax devices (i.e. the MFP models in this evaluation do not contain the Fax Polling Send functionality).

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

The TOE also supports Microsoft SharePoint (*flow* MFP models only) and remote file systems for the storing of scanned documents. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to SharePoint and the remote file systems. For remote file system connectivity, the TOE supports the File Transfer Protocol (FTP) and the Server Message Block (SMB) protocol. (SharePoint is HTTP-based.) The MFP is capable of encrypting stored document files according to the Adobe PDF specification.

The TOE can be used to email scanned documents, email received faxes, or email sent faxes. In addition, TOE can send email alert messages to administrator-specified email addresses, or send automated emails regarding product configuration and MFP supplies to HP. The TOE supports protected communications between itself and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate with the SMTP gateway. 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.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of a touchscreen LCD, and a physical home screen button that are attached to the HCD. In addition, *flow* MFP models include a pull-out keyboard as part of the Control Panel. The Control Panel is the physical interface that a user uses to communicate with the TOE when physically using the HCD. The LCD screen displays information such as menus and status to the user. It also provides virtual buttons to the user such as an alphanumeric keypad for entering usernames and passwords. 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 TOE's Control Panel supports both local and remote sign-in methods. The local sign-in method is called Local Device Sign In which supports individual user accounts. The user account information is maintained in the Local Device Sign In database within the TOE. The remote sign-in methods are called LDAP Sign In and Windows Sign In (i.e., Kerberos). The TOE uses IPsec with X.509v3 certificates to protect both the LDAP and Kerberos communications.

The Scanner in Figure 1 converts hardcopy documents into electronic form. The Print Engine in Figure 1 converts electronic documents into hardcopy form.

All MFP models contain a persistent storage drive (a.k.a. storage drive) that resides in the Operational Environment. The storage drive contains a section called Job Storage which is a user-visible file system where stored print, stored copy, and stored received faxes are stored/held. All MFP models, except the M527dn, contain the HP High-Performance Secure Hard Disk. The M527dn contains eMMC with the HP High-Performance Secure Hard Disk available as an accessory.

If the MFP model contains the HP High Performance Secure Hard Disk, jobs in Job Storage can persist across power-cycles or can be deleted, depending on how the administrator configures the TOE and on the job type. If the MFP model contains an eMMC, all jobs in Job Storage are automatically deleted when the HCD is turned off. (Job types are discussed in section 1.5.4.2.1.)

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 itself and the syslog server and for mutual authentication of both endpoints.

The Jetdirect Inside Firmware and HCD System Firmware components comprise the firmware on the system. They are shown as two separate components but they both share the same operating system (OS). The operating system is part of the Operational Environment. Both firmware components also contain an Embedded Web Server (EWS).

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 TOE's embedded Ethernet interface.

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

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 system and the QuickSec cryptographic library). 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 share the same operating system (which is part of the Operational Environment). The HCD System firmware also includes internal Control Panel 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.

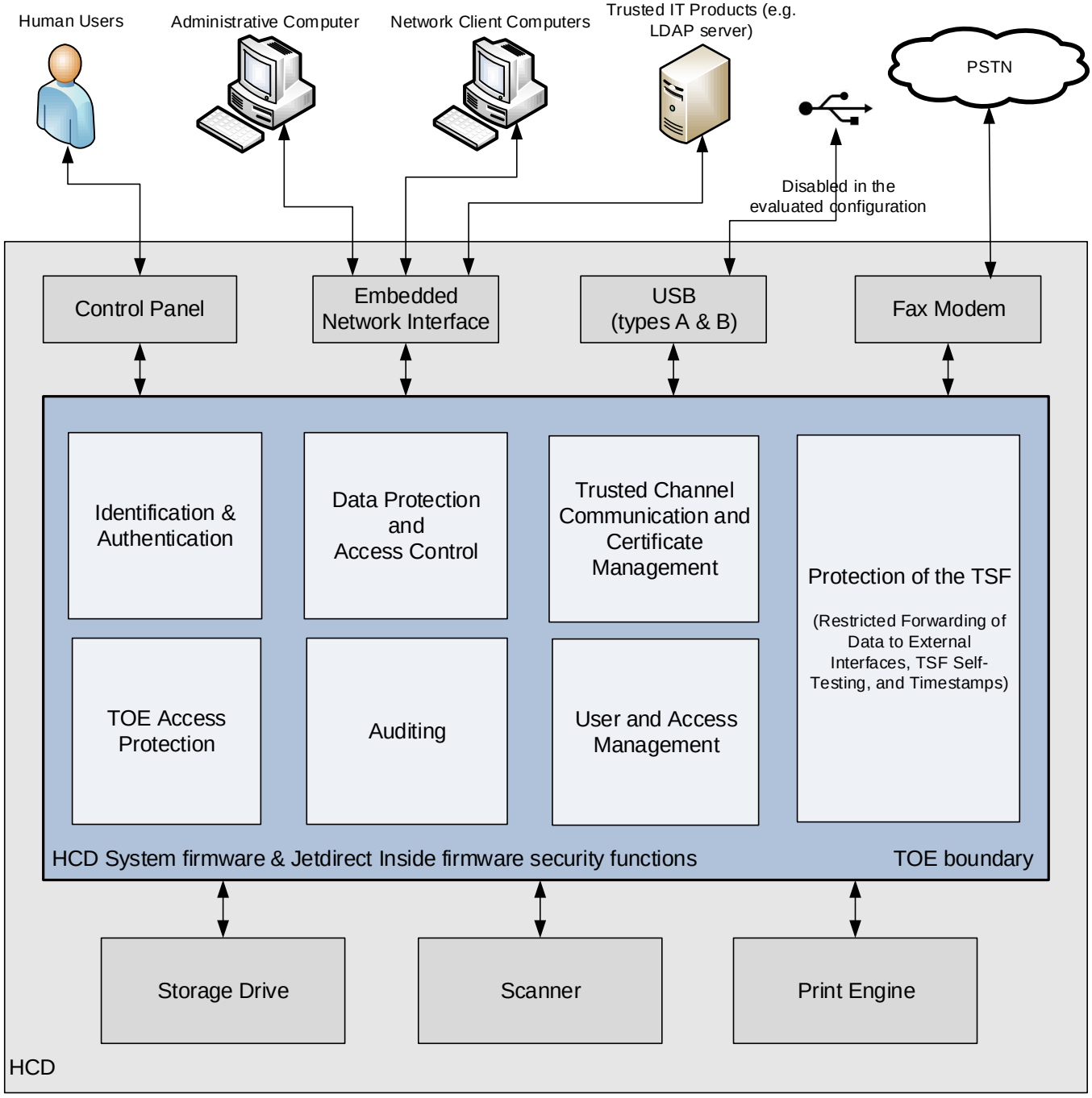

Figure 2: HCD logical diagram

1.5.2 TOE security functionality (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 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec. See section 1.5.2.7 for more information.

The TOE supports the decrypting of print jobs encrypted using the Job Encryption Password. The decryption algorithm used by the TOE for this is included in the TOE. See section 1.5.2.4 for more information.

The product includes functionality to encrypt certain types of scan jobs using the Adobe PDF specification. This encryption functionality is **not** part of the claimed security functions of the TOE. Instead, the TOE uses IPsec to protect its communication channels.

The product includes functionality to encrypt email using S/MIME and X.509v3 certificates. This encryption functionality is **not** part of the claimed security functions of the TOE. Instead, the TOE uses IPsec to protect its communication channels.

1.5.2.2.1 Cryptography outside the scope of the TOE

This section exists to inform the reader that the HCD contains other cryptography that is outside the scope of the TOE, is **not** part of this evaluation, and is **not** used to fulfill any of the [PP2600.2] requirements.

The HP High Performance Secure Hard Disk provides hardware-based cryptography and persistent storage to securely manage sensitive print data. Data on this drive is encrypted and the encryption key is locked to the device. The cryptographic functionality is transparent to the TOE and to the user. Not all MFP models in this evaluation contain this storage drive. The MFP models that do not, instead contain an eMMC.

Certain areas of the eMMC are encrypted under the control of the TOE using the HCD's hardware. Each time the TOE is power-cycled, the cryptographic keys are destroyed and new keys generated to encrypt the storage drive. Because of this, the jobs in Job Storage are effectively erased upon power-cycling the HCD.

1.5.2.3 Identification and authentication

1.5.2.3.1 Control Panel I&A

The HCD has a Control Panel used to select a function (a.k.a. Control Panel application) to be performed. The Control Panel supports both local and remote sign-in methods.

The mechanism for the local sign-in method, which is part of the TOE firmware, is called:

- Local Device Sign In

Remote sign-in methods 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 by the remote sign-in method.

All users must sign in before being presented with the home screen allowing access to Control Panel applications. Prior to signing in, the TOE can be configured to display a Welcome message on which the user must press “OK” before the user can access the sign-in screen. At the sign-in screen, the user may get help on various MFP functions or select a sign-in method prior to signing in. The sign-in method selections are:

- Local Device Sign In:
  - Administrator Access Code
  - User Access Code
- LDAP Sign In (if configured and enabled)
- Windows Sign In (if configured and enabled)

When users sign in 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. The TOE also contains a mechanism called Simplified Account Lockout that slows Control Panel authentication attempts when multiple unsuccessful authentication attempts occur.

1.5.2.3.2 IPsec I&A

Client computers can connect to the TOE to submit print jobs and to manage the TOE. The TOE uses IPsec to identify and mutually authenticate client computers that attempt to connect to the TOE.

The client computers that connect to the TOE are considered IPsec users and are classified as either Network Client Computers or the Administrative Computer. The TOE uses IP addresses to identify these users and X.509v3 certificates to authenticate the users. The IP address of a connecting client computer must be defined in the TOE's IPsec/Firewall in order for the computer to be considered authorized to access the TOE. Any client computer not defined in the TOE's IPsec/Firewall is considered unauthorized and is blocked by the firewall from accessing the TOE.

The TOE uses IPsec/Firewall address templates, service templates, and rules to map IP addresses to network service protocols. An address template contains one or more IP addresses. A service template contains one or more allowed network service protocols. A rule contains a mapping of an address template to a service template. Through the rules, an administrator determines the User Role of the client computers (i.e., the administrator determines which client computer is the Administrative Computer and which client computers are the Network Client Computers). In the evaluated configuration, the IPsec/firewall only allows the Administrative Computer to connect to all interfaces supported by the TOE. The Network Client Computers are limited to just the PJL Interface (TCP port 9100). Table 2 shows the mapping of IPsec users to their allowed network protocols.

IPsec user	Allowed network protocol access
Administrative Computer (U.ADMINISTRATOR)	EWS (HTTP), OXPd, WS*, SNMP, PJL
Network Client Computer (U.NORMAL)	PJL (TCP port 9100 only)

Table 2: IPsec user mappings to allowed network protocols

Because IPsec mutual authentication is performed at the computer level, not the user level, the computer allowed by the firewall to access the TOE via EWS, OXPd, WS*, 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.

IPsec is configured to use X.509v3 certificates via the Internet Key Exchange (IKE) protocols IKEv1 and IKEv2 in the evaluated configuration.

In addition, the TOE can contact many types of trusted IT products 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 email notification to the SMTP Gateway) or to request information from them (e.g., authenticate a user using LDAP). The TOE mutually authenticates these servers via IPsec prior to sending data or requesting information from them.

1.5.2.4 Data protection and access control

1.5.2.4.1 Permission Sets

Each Control Panel application requires one or more permissions in order to execute it. These permissions are defined in Permission Sets (a.k.a. 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 TOE includes a Device Guest Permission Set, but it has zero permissions in the evaluated configuration.

Additional (custom) Permission Sets can be created and applied by the administrator in the evaluated configuration.

In the evaluated configuration, the Device Administrator Permission Set has more permissions than the Device User Permission Set. This translates into U.ADMINISTRATORS users being able to access more functionality, specifically administrative functionality, than U.NORMAL users.

Permission Set data is stored in the TOE and managed via the EWS and WS* Web Services.

1.5.2.4.2 Job PINs

Users control access to print and copy jobs that they place in Job Storage 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 TOE and allow users to control when the jobs are printed so that physical access to the hard copies can be controlled.

1.5.2.4.3 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.

1.5.2.4.4 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 a Job PIN or through the use of just a Job Encryption Password. The user identifier for

a print job received from a client computer is either automatically assigned by that client computer or assigned by the user sending the print job from the client computer. For copy 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

A Control Panel administrator (U.ADMINISTRATOR) user has a permission in their Permission Set that allows the administrator to delete a non-fax job in Job Storage.

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 received fax jobs in Job Storage.

1.5.2.4.5 TOE function access control

For Control Panel users, the TOE controls access to Control Panel applications (e.g., Retrieve from Device Memory) using Permission Sets and, optionally, sign-in methods (authentication databases). Permission Sets act as User Roles to determine if the user can perform a function controlled by permissions.

Each Control Panel application requires the user to have one or more specific permissions in their session Permission Set in order to access that application. In addition, the TOE's administrator can map a sign-in method to each Control Panel application and require the user to be authenticated to that sign-in method in order to access that application. The individual applications only check and enforce permissions. They do not check the sign-in methods. Instead, the TOE enforces the sign-in method requirement at the time that the user signs in to the TOE by removing permissions from the user's session Permission Set for each application in which the user's sign-in method does not match the sign-in method required by the TOE. By removing the permissions required by each non-matching application, the TOE limits the set of applications that the user can access.

Administrators can change/modify the sign-in method mapped to each application. In addition, the TOE contains a function that allows administrators to select if the sign-in method application mappings are enforced or ignored by the TOE. This function is called "Allow users to choose alternate sign-in methods." When this function is disabled, the TOE enforces the "sign in method to application" mappings and prunes (reduces) the user's session Permission Set accordingly. When this function is enabled, the sign in method mappings are ignored by the TOE and the user's session Permission Set remains unchanged.

For IPsec users, the TOE uses the IPsec/Firewall to control access to the supported network service protocols. The IPsec/Firewall contains the IP addresses of authorized client computers grouped into address templates and the network service protocols grouped into service templates. The administrator maps an address template to a service template using an IPsec/Firewall rule. Service templates, therefore, act as the User Roles. IP addresses of computers not contained in a rule are denied access to the TOE.

1.5.2.4.6 Residual information protection

The TOE protects deleted objects by making them unavailable to TOE users via the TOE's interfaces. This prevents TOE users from attempting to recover deleted objects of other users via the TOE interfaces.

1.5.2.5 Protection of the TSF

1.5.2.5.1 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 feature Fax Archive, which can automatically archive faxes, can be enabled/disabled by an administrator. The administrator can control the destination of the archived fax data. The TOE does not provide a pathway or support for commands necessary to achieve network access.

1.5.2.5.2 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.

1.5.2.5.3 Reliable timestamps

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

1.5.2.6 TOE access protection

1.5.2.6.1 Inactivity timeout

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

1.5.2.6.2 Automatic logout

The Control Panel supports the following administrator-selectable automatic logout functions:

- Sign out the user immediately after starting the job
- Sign out the user 10 seconds after starting the job with the user-selectable option to remain signed in

If the user signs in and never starts a job, the inactivity timeout feature will terminate the session.

1.5.2.7 Trusted channel communication and certificate management

The TOE supports IPsec to protect data being transferred over the Shared-medium Interface. IPsec uses IP addresses and X.509v3 certificates to identify and authenticate the Network Client Computers and the Administrative Computer as well as other trusted IT products to which the TOE connects (e.g., syslog server, SMTP gateway).

The TOE uses several cryptographic algorithms with IPsec. These cryptographic algorithms, supplied by the QuickSec cryptographic library, are all part of the Operational Environment, but the TOE controls the usage of these algorithms. Also, the TOE uses a software-based random number generator in the Operational Environment 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 manage (add, replace, delete) X.509v3 certificates.

1.5.2.8 User and access management

The TOE provides management capabilities for managing its security functionality. The TOE supports the following roles:

- administrators (U.ADMINISTRATOR)
- users (U.NORMAL)

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

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 system and the QuickSec cryptographic library) and the English-language guidance documentation.

It is typical for an HCD, and thus the TOE, to be shared by many users and for those users to have direct physical access to the HCD. By design, users have easy access to some of the hardware features, such as the Control Panel, the paper input trays, the paper output trays, the scanner, and the power button. But other features such as the processor, volatile memory, and storage drive are located inside the HCD in the formatter cage. The formatter cage can be secured to the HCD chassis using a combination lock, thus, restricting normal user access to the components inside the cage.

Because of the restricted access to the storage drive, the drive is considered a non-removable non-volatile 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.

QuickSec version 5.1 ([QuickSec51]) library implements the TOE's IPsec including the IPsec/Firewall. QuickSec includes a cryptographic library. Although the IPsec implementation in QuickSec is in the TOE boundary, the QuickSec cryptographic library used by QuickSec for all IPsec cryptography is part of the Operational Environment. QuickSec is developed and tested by INSIDE Secure.

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 table lists the English-guidance documentation for the TOE:

Title	Edition
Common Criteria Evaluated Configuration Guide for HP LaserJet Enterprise MFP M527 Series, Color LaserJet Enterprise MFP M577 Series, and PageWide Enterprise Color MFP 586 Series	1
HP LaserJet Enterprise MFP M527 User Guide	1
HP Color LaserJet Enterprise MFP M577 User Guide	1
HP PageWide Enterprise Color MFP 586 User Guide	1

Table 3: English-only guidance documentation

1.5.3.2 Logical

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

- Auditing
- Cryptography

- Identification and authentication
- Data protection and access control
- Protection of the TSF (restricted forwarding, TSF self-testing, and timestamps)
- TOE access protection (inactivity timeout and automatic logout)
- Trusted channel communication and certificate management
- User and access management

1.5.3.3 **Evaluated configuration**

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

- HP Digital Sending Software (DSS) must be disabled
- Device Administrator Password must be set as per P.ADMIN.PASSWORD
- Only one Administrative Computer is used to manage the TOE
- HP and third-party applications cannot be installed on the TOE
- All non-fax stored jobs must be assigned a Job PIN or encrypted with a password
- All received faxes (excluding Fax Polling Receive jobs) must be stored in Job Storage
- PC Fax Send must be disabled
- Type A and B USB ports must be disabled
- Remote Firmware Upgrade through any means other than the EWS (e.g., PJL) and USB must be disabled
- Jetdirect Inside management via telnet and FTP must be disabled
- Jetdirect XML Services must be disabled
- File System External Access must be disabled
- IPsec authentication using X.509v3 certificates must be enabled (IPsec authentication using Kerberos or Pre-Shared Key is not supported)
- IPsec Authentication Headers (AH) must be disabled
- Full Authentication must be enabled (this disables the Guest role)
- 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 HP support personnel, must be disabled
- Near Field Communication (NFC) must be disabled
- Wireless Direct Print must be disabled
- PJL device access commands must be disabled
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections

- The “Save to HTTP” function is disallowed and must not be configured to function with an HTTP server
- Display Names for the Local Device Sign In method users and user names for the LDAP and Windows Sign In method users must only contain the characters defined in P.USERNAME.CHARACTER_SET
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.DISALLOWED

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 4.

<table>
<tr><th>Designation</th><th colspan="2">Definition</th></tr>
<tr><td rowspan="3">U.USER</td><td colspan="2">Any authorized User. Authorized Users are U.ADMINISTRATOR and U.NORMAL.</td></tr>
<tr><td>Designation</td><td>Definition</td></tr>
<tr><td>U.NORMAL</td><td>A User who is authorized to perform User Document Data processing functions of the TOE.</td></tr>
<tr><td></td><td>U.ADMINISTRATOR</td><td>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.</td></tr>
</table>

Table 4: 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 the TOE's Control Panel.
  - **Security attributes:** User Role (defined by Permission Set) and User Identifier
- **Incoming analog fax phone line users** – Unauthenticated entities that initiate and transmit faxes to the TOE over the TOE’s analog fax phone line connection. 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
- **IPsec users:**
  - **Network Client Computers** – Computers (U.NORMAL entities) that can successfully authenticate to the TOE's PJL Interface (TCP port 9100) using IPsec and mutual

authentication. The TOE will accept print jobs from any user of a client computer where the client computer has successfully authenticated with the TOE.

- **Security attributes:** User Role (defined by IPsec/Firewall service template) and User Identifier (defined by IP address)

- **Administrative Computers** – Computers (U.ADMINISTRATOR entities) that can successfully authenticate to the TOE's administrative interfaces (e.g., EWS/HTTP, OXPd, WS*, SNMP) using IPsec and mutual authentication. An Administrative Computer may also connect to the TOE 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 IPsec/Firewall service template) and User Identifier (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.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

Table 5: User Data

User Data objects include:

- **Fax jobs:**
  - **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. For PIN protected stored jobs, the user must be the job owner or know the Job PIN (or have administrator privileges) in order to delete the job. These jobs are automatically deleted after printing or if the HCD is turned off or after an administrator specified time interval. If the HCD contains the HP High Performance Secure Hard Disk, the administrator can configure the TOE to retain these jobs over a power cycle.
    - **Stored jobs** – Print jobs such as a personnel form, time sheet, or calendar from a client computer that are stored on the TOE and reprinted. In the evaluated configuration, such jobs must be PIN protected with a Job PIN. The administrator can configure the TOE to automatically delete these jobs after a specified time interval. For PIN protected stored jobs, the user must be the job owner or know the Job PIN (or have administrator privileges) in order to delete the job. If the HCD contains an eMMC, these jobs are automatically deleted when the HCD is turned off.
    - **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. If the HCD contains an eMMC, these jobs are automatically deleted when the HCD is turned off.
- **Scan job types:**
    - **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.
    - **Save to SharePoint jobs** – Scan jobs that are saved to a SharePoint server.
- **Stored copy jobs** – A copy job that a Control Panel user has stored on the TOE. 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 TOE. 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

Designation	Definition
	of the TOE, but for which disclosure is acceptable.

Table 6: 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 (including IPsec/Firewall rules and templates)		X
Job data including Job PINs	X	
PJL protocol excluding the 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 7: 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
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

Designation	Definition
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 8: 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	Indicated 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 9: 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])

In this Security Target, [PP2600.2] has been modified to conform with the NIAP CCEVS Policy Letter #20 ([CCEVS-PL20]).

Although the HCDs in this Security Target contain a nonvolatile mass storage device (i.e., a storage 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". The term "common" is used to refer to that portion of [PP2600.2] to which all TOEs must conform (i.e., the portions not labeled as packages).

[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

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
				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			The TOE's Control Panel supports authentication (FIA_UAU.1).
	FIA_UAU.2		X	The TOE supports IPsec authentication (FIA_UAU.2) which

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
				complies with the more restrictive FIA_UAU.2.
FIA_UID.1	FIA_UID.1			The TOE's Control Panel supports identification (FIA_UID.1).
	FIA_UID.2		X	The TOE supports IPsec identification (FIA_UID.2) which complies with the more restrictive FIA_UID.2.
FIA_USB.1	FIA_USB.1			n/a
FMT_MSA.1(a)	FMT_MSA.1-perm	X		FMT_MSA.1(a) iteration name is different to better reflect the security attributes involved because this SFR is shared with another access control policy.
FMT_MSA.1(b)	FMT_MSA.1-perm and FMT_MSA.1-tfac	X		FMT_MSA.1(b) was further iterated because the operations on the security attributes 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

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
FMT_SMR.1	FMT_SMR.1			n/a
FPT_STM.1	FPT_STM.1			n/a
FPT_TST.1	FPT_TST.1			n/a
FTA_SSL.3	FTA_SSL.3			n/a

Table 10: 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
None	FCS_CKM.1			FCS_CKM.1 specifies the types of cryptographic keys generated by the TOE for use with AES and HMAC in IPsec.
None	FCS_CKM.2			FCS_CKM.2 specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec.
None	FCS_COP.1-ipsec	X		FCS_COP.1-ipsec specifies the AES encryption and decryption algorithm, the RSA decryption algorithm, and the HMAC algorithms used by the TOE in IPsec.
None	FCS_COP.1-job	X		FCS_COP.1-job specifies the AES decryption algorithm used by the TOE for decrypting encrypted print jobs.
None	FIA_AFL.1			The TOE slows the number of unsuccessful Control Panel authentication attempts made over a period of time. Recommended by [PP2600.2] APPLICATION NOTE 38.
None	FIA_SOS.1			FIA_SOS.1 specifies the Job PIN strength of certain authorization

[PP2600.2] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
				mechanisms used by the TOE.
None	FIA_UAU.7			The TOE masks Job PINs, Access Codes, and passwords. Recommended by [PP2600.2] APPLICATION NOTE 38.
None	FMT_MOF.1-auth	X		The TOE allows administrators to allow or disallow users from choosing an alternate sign in method differing from the administrator-selected method.
None	FMT_MOF.1-faxarchive	X		The TOE allows the administrator to allow or disallow use of the Fax Archive feature.

Table 11: 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 12: 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 13: 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 14: SFR mapping 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 15: 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 16: 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 17: 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.SERVICES.RELIABLE

When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services provide reliable information and responses to the TOE.

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.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), WS* Web Services, OXPd Web Services, and at the Control Panel.

P.USERNAME.CHARACTER_SET

To prevent ambiguous user names in the TOE's audit trail, the Display Names of the Local Device Sign In method users and the user names of the LDAP and Windows Sign In method users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

P.REMOTE_PANEL.DISALLOWED

To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature.

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.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.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.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.SERVICES.RELIABLE

When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services shall provide reliable information and responses 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.PC.POLICY

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

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.USERNAME.CHARACTER_SET

The Display Names of all Local Device Sign In method users and the user names of all LDAP and Windows Sign In method users shall only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

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

Objective	Threats / OSPs
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 18: 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.PC.SECURE	A.ADMIN.PC.SECURE
OE.ADMIN.TRAINED	A.ADMIN.TRAINING P.ADMIN.PASSWORD P.REMOTE_PANEL.DISALLOWED
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

Objective	Assumptions / Threats / OSPs
OE.PHYSICAL.MANAGED	A.ACCESS.MANAGED
OE.SERVICES.RELIABLE	A.SERVICES.RELIABLE
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.PC.POLICY	A.USER.PC.POLICY
OE.USER.TRAINED	A.USER.TRAINING
OE.USERNAME.CHARACTER_SET	P.USERNAME.CHARACTER_SET

Table 19: 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

Threat	Rationale for security objectives
	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. • 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

Threat	Rationale for security objectives
	appropriately grant authorization.

Table 20: 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: • 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

Assumption	Rationale for security objectives
	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.TRUSTED which establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.SERVICES.RELIABLE	The assumption: • When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services provide reliable information and responses to the TOE. is upheld by: • OE.SERVICES.RELIABLE which, when the TOE uses the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, establishes that these services provide reliable information and responses to the TOE.

Table 21: 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

OSP	Rationale for security objectives
	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. 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

OSP	Rationale for security objectives
	protected environment for TOE external interfaces.
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), WS* Web Services, OXPd Web Services, and at the Control Panel. is enforced by: • OE.ADMIN.TRAINED which establishes responsibility of the TOE Owner to provide appropriate Administrator training.
P.USERNAME.CHARACTER_SET	The OSP: • To prevent ambiguous user names in the TOE's audit trail, the Display Names of the Local Device Sign In method users and the user names of the LDAP and Windows Sign In method users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E). is enforced by: • OE.USERNAME.CHARACTER_SET which establishes that the Display Names of all Local Device Sign In users and the user names of all LDAP and Windows Sign In methods users shall only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).
P.REMOTE_PANEL.DISALLOWED	The OSP: • To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature. is enforced by: • OE.ADMIN_TRAINED which establishes responsibility of the TOE Owner to provide appropriate Administrator training.

Table 22: 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 Cryptographic key generation		CC Part 2	No	Yes	Yes	No
	FCS_CKM.2 Cryptographic key distribution		CC Part 2	No	Yes	Yes	No
	FCS_COP.1-ipsec Cryptographic operation	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_COP.1-job 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

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_AFL.1 Authentication failure handling		CC Part 2	No	No	Yes	Yes
	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		CC Part 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		CC Part 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-faxarchive Management of Fax Archive security	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	functions behavior						
	FMT_MSA.1-perm Management of Permission Set 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
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 23: 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 24: Auditable Events: 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 24: Auditable Events: (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]
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1, FIA_UAU.2	Basic	None required	Yes: Common
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1, FIA_UID.2	Basic	Attempted user identity, if available	Yes: Common
Use of the management functions	FMT_SMF.1	Minimum	None required	Yes: Common
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required	Yes: Common
Changes to the time	FPT_STM.1	Minimum	None required	Yes: Common
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required	Yes: SMI

Termination of an interactive session by the session termination mechanism	FTA_SSL.3	Minimum	None required	No

Table 24: 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)

FCS_CKM.1.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in Table 25: Cryptographic key generation** and specified cryptographic key sizes **defined in Table 25: Cryptographic key generation** that meet the following: **the standards defined in Table 25: Cryptographic key generation**.

Protocol	Key generation algorithm	Key sizes (in bits)	Standards
IPsec	AES	128, 192, 256	[RFC4301] Security Architecture for the Internet Protocol
	HMAC-SHA1-96	96	[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
	HMAC-SHA-256-128	256	[RFC4868] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
	HMAC-SHA-384-196	384	
	HMAC-SHA-512-256	512	

Table 25: Cryptographic key generation

Application Note: *Key generation for FCS_CKM.1 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 distribution (FCS_CKM.2)

FCS_CKM.2.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **defined in Table 26: Cryptographic key distribution** that meets the following: **the standards defined in Table 26: Cryptographic key distribution**.

Protocol	Key distribution method	Standards
IPsec	IKEv1	[RFC2409] The Internet Key Exchange (IKE); [RFC4109] Algorithms for Internet Key Exchange version 1 (IKEv1)
	IKEv2	[RFC4306] Diffie-Hellman key agreement method defined for the IKEv2 protocol; [RFC4718] IKEv2 Clarifications and Implementation Guidelines

Table 26: Cryptographic key distribution

6.1.2.3 Cryptographic operation (FCS_COP.1-ipsec)

FCS_COP.1.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall perform **the operations defined in Table 27: Cryptographic operations** in accordance with a specified cryptographic algorithm **defined in Table 27: Cryptographic operations** and cryptographic key sizes **defined in Table 27: Cryptographic operations** that meet the following: **the standards defined in Table 27: Cryptographic operations**.

Protocol	Operations	Algorithm	Key sizes (in bits)	Standards
IPsec	Asymmetric decryption	RSA	1024, 2048, 4096	[PKCS1v1.5] Public-Key Cryptography Standard (PKCS) #1: RSA Encryption Standard
	Symmetric encryption and decryption	AES (CBC mode)	128, 192, 256	[FIPS197] Advanced Encryption Standard; [SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques
	Data authentication	HMAC-SHA1-96	96	[RFC2104] HMAC: Keyed-Hashing for Message Authentication

		HMAC-SHA-256-128	256	[RFC4868] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
		HMAC-SHA-384-192	384	
		HMAC-SHA-512-256	512	

Table 27: Cryptographic operations

6.1.2.4 Cryptographic operation (FCS_COP.1-job)

FCS_COP.1.1 The TSF shall perform **the operations defined in Table 28: Cryptographic operations** in accordance with a specified cryptographic algorithm **defined in Table 28: Cryptographic operations** and cryptographic key sizes **defined in Table 28: Cryptographic operations** that meet the following: **the standards defined in Table 28: Cryptographic operations**.

Protocol	Operations	Algorithm	Key sizes (in bits)	Standards
Print job	Symmetric decryption	AES (CBC mode)	256	[FIPS197] Advanced Encryption Standard; [SP800-38A] Recommendation for Block Cipher Modes of Operation

Table 28: Cryptographic operations

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 29: Common Access Control SFP** on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 29: Common Access Control SFP**.

Object	Operation(s)	Subject	Access control rules	[PP2600.2] section
D.FUNC	Modify, Delete	U.NORMAL	For stored print and stored copy 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 Job Storage permission in their Permission Set to delete the job; otherwise, delete access is denied.	Common

			D.FUNC for Stored Jobs cannot be modified by any user, including U.ADMINISTRATOR. For encrypted stored print jobs in Job Storage: From the Control Panel, subjects must know the job's Job Encryption Password or have the appropriate Job Storage permission in their Permission Set to delete D.FUNC; otherwise, delete access is denied. For Receive Fax jobs in Job Storage: 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.	
D.DOC	Delete	U.NORMAL	For stored print and stored copy 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 Job Storage permission in their Permission Set to delete the job; otherwise, delete access is denied. For encrypted stored print jobs in Job Storage: From the Control Panel, subjects must know the job's Job Encryption Password or have the appropriate Job Storage permission in their Permission Set to delete D.DOC; otherwise, delete access is denied. For Receive Fax jobs in Job Storage: 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.)	Common

			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.	
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 stored 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 in Job Storage: Subjects must know the job's Job Encryption Password to read the object, otherwise, read access is denied.	DSR, PRT
D.DOC+DSR D.DOC+FAXIN D.DOC+FAXOUT	Read	U.NORMAL	(D.DOC+FAXIN+DSR) For Receive Fax jobs in Job Storage: 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	CPY

			access.	

Table 29: 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 29: Common Access Control SFP** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 29: Common Access Control SFP, and for each, the indicated security attributes in Table 29: Common Access Control SFP** .

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 29: Common Access Control SFP 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:

- **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:**

- **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**
  - **Association of a sign in method to a Control Panel application**
- **Users: Network Client Computers, Administrative Computer;**
  Functions: F.DSR, F.PRT, F.SMI;
  Security attributes:
  - **User Role as defined by the user's IPsec/Firewall service templates.**

Application Note: *The "Allow users to choose alternate sign-in methods" function affects the sign in processing behavior of Control Panel users, but is considered a function instead*

of a security attribute and, thus, not listed under "security attributes" above.

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

- **The user is explicitly authorized by U.ADMINISTRATOR to use a function**
- **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 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 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **the Number for the specified Sign In method in Table 30: Simplified Account Lockout for each sign in method of** unsuccessful authentication attempts occur related to **the Event for the same Sign In method in Table 30: Simplified Account Lockout for each sign in method**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **perform the Action for the same Sign In method in Table 30: Simplified Account Lockout for each sign in method**.

Application Note: *Multiple unsuccessful authentication attempts using the same authentication data are counted as just one unsuccessful authentication attempt by the sign in methods. For example, assuming the LDAP Sign In method has zero unsuccessful authentication attempts, if the same user types the same incorrect password into the LDAP Sign In method seven times in a row, the sign in method will only count it as one unsuccessful authentication attempt*.

Sign In method	Number	Event	Action
Local Device Sign In: Administrator Access Code	6	the latest successful authentication for the Administrator Access Code	insert a 10 second delay between each Administrator Access Code authentication attempt until: • a successful Administrator Access Code authentication occurs, or • 5 minutes elapses after the last failed Administrator Access Code authentication

Sign In method	Number	Event	Action
Local Device Sign In: User Access Code	6	the last successful authentication for User Access Code sign in method (i.e., per method, not per Access Code)	insert a 10 second delay between all User Access Code authentication attempts until: • any successful User Access Code authentication occurs, or • 5 minutes elapses after the last failed authentication of all User Access Codes
LDAP Sign In	6	the last successful authentication for the indicated LDAP Sign In user	insert a 10 second delay between authentication attempts of the indicated user until: • a successful authentication of the indicated user occurs, or • 5 minutes elapses after the last failed authentication attempt of the indicated user
Windows Sign In	6	the last successful authentication for the indicated Windows Sign In user	insert a 10 second delay between authentication attempts of the indicated user until: • a successful authentication of indicated user occurs, or • 5 minutes elapses after the last failed authentication attempt of the indicated user

Table 30: Simplified Account Lockout for each sign in method

6.1.4.2 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:

- **Control Panel users:**
  - **User Identifier (Access Code and Display Name) for Local Device Sign In**
  - **User Role (defined by Permission Set)**
- **IPsec users:**
  - **User Identifier (defined by IP address)**
  - **User Role (defined by IPsec/Firewall service template)**

Application Note: *The LDAP and Windows Sign In method security attributes belonging to individual users are not in FIA_ATD.1 because these attributes are "maintained" independently by the LDAP server and Windows domain controller, respectively, which are part of the Operational Environment*.

6.1.4.3 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the requirement: Job PINs shall be 4 digits**.

6.1.4.4 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 a sign in method** 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.

6.1.4.5 IPsec authentication before any action (FIA_UAU.2)

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

6.1.4.6 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**
- **Authentication password character typed**
- **Job PIN digit typed**

to the user while the *Control Panel* authentication is in progress.

Application Note: *Job PINs are not used for authentication, but the digits are masked when entered*.

6.1.4.7 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 a sign in method** 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.

6.1.4.8 IPsec identification before any action (FIA_UID.2)

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

6.1.4.9 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **User Identifier (Display Name for Local Device Sign In, user name for both LDAP Sign In and Windows Sign In, IP address for IPsec) and User Role**.

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users: **If "Allow users to choose alternate sign-in methods" is disabled, the user's session Permission Set will be reduced to exclude the permissions of applications whose sign in method does not match the sign in method used by the user to sign in.**

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 **enable, disable** the functions **"Allow users to choose alternate sign-in methods" for Control Panel applications** to **U.ADMINISTRATOR**.

6.1.5.2 Management of Fax Archive security functions behavior (FMT_MOF.1-faxarchive)

FMT_MOF.1.1 The TSF shall restrict the ability to **enable, disable** the functions **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 29: Common Access Control SFP and TOE Function Access Control SFP** to restrict the ability to **modify, create, delete** the security attributes **Permission Sets and Permission Set associations** to **U.ADMINISTRATOR**.

Application Note: *The rule applies to all the Permission Sets except the Device Administrator and Device User. These default Permission Sets cannot be created, renamed or deleted. In addition, the permissions in Device Administrator Permission Set cannot be modified.*

6.1.5.4 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

- **IPsec/Firewall service templates (defining IPsec User Roles): create, modify,**

delete operations

- **Association of a sign in method to a Control Panel application: modify operation**

to **U.ADMINISTRATOR**.

6.1.5.5 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

- **IPsec CA X.509v3 certificate: add, replace, delete operations**
- **IPsec identity X.509v3 certificate: replace operation**
- **IPsec/Firewall address templates and rules for IPsec users: create, modify, delete operations**
- **IPsec/Firewall address templates, service templates, and rules for trusted IT products: create, modify, delete operations**

to **U.ADMINISTRATOR**.

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

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

6.1.5.7 Specification of management functions (FMT_SMF.1)

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

- **Fax archive management (FMT_MOF.1-faxarchive)**
- **IPsec/Firewall rules, address templates, and service templates management (FMT_MSA.1-tfac, FMT_MTD.1-auth)**
- **IPsec X.509v3 certificate management (FMT_MTD.1-auth)**
- **Local Device Sign In data (Access Code) management (FMT_MTD.1-users)**
- **Permission Set management (FMT_MSA.1-perm)**
- **Sign in method association management (FMT_MOF.1-auth, FMT_MSA.1-tfac).**

6.1.5.8 Security roles (FMT_SMR.1)

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

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

- **Local Device Sign In - User Access Code verification**
- **LDAP Sign In - LDAP Settings verification**
- **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

- **Local Device Sign In database**
- **Device Administrator Password**
- **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:*

- **The user starts any job (if configured by U.ADMINISTRATOR)**
- **10 seconds after a user starts any job and the user agrees to the termination (if configured by U.ADMINISTRATOR)**
- **20 seconds 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
FAU_GEN.2	O.AUDIT.LOGGED
FCS_CKM.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
FCS_CKM.2	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	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	O.DOC.NO_ALT,

Security functional requirements	Objectives
	O.DOC.NO_DIS
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
FDP_RIP.1	O.DOC.NO_DIS
FIA_AFL.1	O.USER.AUTHORIZED
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,

Security functional requirements	Objectives
	O.PROT.NO_ALT, O.USER.AUTHORIZED
FIA_USB.1	O.USER.AUTHORIZED
FMT_MOF.1-auth	O.PROT.NO_ALT
FMT_MOF.1-faxarchive	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-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

Security functional requirements	Objectives
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 31: 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: • 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 which specifies the type of cryptographic keys generated by the TOE for use with HMAC algorithms in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the RSA decryption algorithms and HMAC algorithms used by the TOE. • 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

Security objectives	Rationale
	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: • FCS_CKM.1 which specifies the type of cryptographic keys generated by the TOE for use with AES in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the AES encryption/decryption algorithms and the RSA decryption algorithms used by the TOE in IPsec. • 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 which specifies the type of cryptographic keys generated by the TOE for use with HMAC algorithms in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution

Security objectives	Rationale
	methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the RSA decryption algorithms used by the TOE and the HMAC algorithms used by the TOE in IPsec. • FCS_COP.1-job which specifies the AES decryption algorithm used by the TOE to process encrypted jobs. • FDP_ACC.1-cac which enforces protection by establishing an access control policy. • FDP_ACF.1-cac which supports access control policy by providing access control function. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm which supports 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 which specifies the type of cryptographic keys generated by the TOE for use with AES in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the AES encryption/decryption algorithms and the RSA decryption algorithms used by the TOE in IPsec. • FCS_COP.1-job which specifies the AES decryption algorithm used by the TOE to process encrypted jobs. • FDP_ACC.1-cac which enforces protection by establishing an access control policy. • FDP_ACF.1-cac which supports access control policy by providing access control function. • FDP_RIP.1 which enforces protection by making residual data unavailable.

Security objectives	Rationale
	• FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm which supports 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.FUNC.NO_ALT	The objective: • The TOE shall protect User Function Data from unauthorized alteration. is met by: • FCS_CKM.1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC algorithms in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the RSA decryption algorithms used by the TOE and the HMAC algorithms 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. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1-perm which supports 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

Security objectives	Rationale
	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-faxarchive which allows the administrator to allow or disallow use of the Fax Archive feature. • FPT_FDI_EXP.1 which enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces. • FTA_SSL.3 which enforces management of external interfaces by terminating inactive sessions.
O.PROT.NO_ALT	The objective: • The TOE shall protect TSF Protected Data from unauthorized alteration. is met by: • FCS_CKM.1 which specifies the type of cryptographic keys generated by the TOE for use with HMAC algorithms in IPsec. • FCS_CKM.2 which specifies the cryptographic key distribution methods used by the TOE in IKEv1 and IKEv2 in IPsec. • FCS_COP.1-ipsec which specifies the RSA decryption algorithm and the HMAC algorithms used by the TOE in IPsec. • 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 the selection of sign in methods. • 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

Security objectives	Rationale
	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: • 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_AFL.1 which slows the number of unsuccessful Control Panel authentication attempts made over a period of time. • 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 32: 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	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2 FCS_COP.1-ipsec
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms of the operating system prevent their use except in the intended context.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The distributed symmetric keys are not formally destroyed. The object reuse mechanisms in the operating system prevent their use except in the intended context.
FCS_COP.1-ipsec	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	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 operating system prevent their use except in the intended context.
FCS_COP.1-job	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. The Network Client Computer encrypts the print job prior to sending the print job to the TOE using an AES 256-bit key derived from the user's Job Encryption Password. The TOE requires the Control Panel user to reenter the same Job Encryption Password so that the TOE can derive the same AES 256-bit key in order to decrypt the print job.
	FCS_CKM.4	This dependency is unresolved. The key used for decryption is not formally destroyed. The object reuse mechanisms in the operating system prevent their use except in the intended context.

Security functional requirement	Dependencies	Resolution
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, 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 service templates, associations of sign in method to a Control Panel application, and Permission Sets do not have default values and do not allow for the specification of alternative initial values.
FDP_RIP.1	No dependencies.	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
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-	FMT_SMR.1	FMT_SMR.1

Security functional requirement	Dependencies	Resolution
faxarchive	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-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.	
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 33: TOE SFR dependency analysis

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
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

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	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 34: 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 TOE. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Auditing
- Cryptography
- 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 HCD 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 subject identity used in the audit record is formed in the following manner. For Local Device Sign In, the subject's identity contains the user's Display Name prefixed with "LOCAL\". For LDAP Sign In, the subject's identity contains the user's LDAP user name prefixed with either the LDAP server's host name or IP address then a backslash. For Windows Sign In, the subject's identity contains the user's Windows domain name and Windows user name separated by a "\". For IPsec, the subject's identity is the user's IP address.

The time source used for the audit record timestamps is discussed in section 7.1.5.3.

This section maps to the following SFRs:

- FAU_GEN.1
- FAU_GEN.2

7.1.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec. See section 7.1.6.27 for more information.

The TOE supports the decrypting of print jobs encrypted using the Job Encryption Password. The decryption code used by the TOE is included in the TOE. See section 7.1.4.3 for more information.

7.1.3 Identification and authentication (I&A)

The TOE supports multiple Control Panel sign in methods, both local and remote methods. It also supports IPsec identification and mutual authentication.

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)

7.1.3.1 **Control Panel I&A**

The Control Panel interface supports both local and remote sign in methods. The following sign in methods are allowed with the evaluated configuration:

- Local sign in method:
  - Local Device Sign In
- Remote sign in methods:
  - LDAP Sign In
  - Windows Sign In (via Kerberos)

(The servers for the remote sign in methods 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 MFP functions.

The TOE contains a local user database for defining non-administrative (U.NORMAL, by default) device user and administrative (U.ADMINISTRATOR) device user accounts used to support the Local Device Sign In mechanism. Each device user account contains the following security attributes:

- Access Code (8 digits)
- Display Name
- Permission Set

The Access Code is a number that serves as both the login 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.

The Display Name is a unique name assigned to the account by the administrator. This name is a security attribute because it is used in audit records to identify the user. (The Access Code is not written in the audit records.)

The Permission Set defines/determines a user's access to many of the TOE's functions. Permission Sets are discussed in more detail in section 7.1.4.1.

Like Local Device Sign In, the remote sign-in methods are used by the Control Panel. The TOE receives authentication credentials from the Control Panel users and passes the credentials to the remote sign-in method. The remote sign in method 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 Windows domain controller. The user must have a valid and active Windows domain 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 an asterisk character of a PIN, Access Code, or password typed to prevent onlookers from viewing another user's authentication data. (Job PINs are not authentication data, but the Job PIN is masked.)

The TOE contains a feature called Simplified Account Lockout to help protect against brute-force attacks at the Control Panel. Each Control Panel sign-in method performs its Simplified Account Lockout independent of the other Control Panel sign-in methods.

The Administrator Access Code method inserts a 10 second delay between each Administrator Access Code authentication attempt upon reaching 6 failed attempts. It keeps inserting the delay until either:

- a valid Administrator Access Code is entered, or
- 5 minutes elapses after the last failed Administrator Access Code authentication attempt.

The User Access Code method inserts a 10 second delay between each User Access Code authentication attempt upon reaching 6 failed attempts. The failed attempts count cumulative for the entire method, not per Access Code. It keeps inserting the delay until either:

- a valid User Access Code is entered, or
- 5 minutes elapses after all failed User Access Code authentication attempts.

The LDAP Sign In method inserts a 10 second delay between each authentication attempt by the same LDAP user upon reaching 6 failed attempts. It keeps inserting the delay until either:

- the indicated LDAP user successfully authenticates, or
- 5 minutes elapses after the last failed authentication attempt by the indicated LDAP user.

Like the LDAP Sign In method, the Windows Sign In method inserts a 10 second delay between each authentication attempt by the same Windows user upon reaching 6 failed attempts. It keeps inserting the delay until either:

- the indicated Windows user successfully authenticates, or
- 5 minutes elapses after the last failed authentication attempt by the indicated Windows user.

Multiple unsuccessful authentication attempts using the same authentication data are counted as just one unsuccessful authentication attempt by the sign in methods. For example, assuming the LDAP Sign In method has zero unsuccessful authentication attempts, if the same user types the same incorrect password into the LDAP Sign In method seven times in a row, the sign in method will only count it as one unsuccessful authentication attempt.

This section maps to the following SFRs:

- FIA_AFL.1
- FIA_ATD.1
- FIA_UAU.1
- FIA_UAU.7
- FIA_UID.1
- FIA_USB.1
- FMT_SMR.1

7.1.3.2 **IPsec I&A**

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

- Administrative Computer (U.ADMINISTRATOR)
- Network Client Computers (U.NORMAL)

IPsec uses IP addresses and X.509v3 certificates via the IKE protocols (IKEv1 and IKEv2) to identify and authenticate, respectively, a client computer. The TOE contains one X.509v3 identity certificate and one or more X.509v3 CA certificates to use for the IPsec mutual authentication. The TOE does not maintain individual X.509v3 certificates of its client computers.

The User Identity of a client computer is its IP address. The TOE's internal firewall maintains lists (IPsec/Firewall address templates) 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 IP address that is not defined in the IPsec/Firewall as either the Administrative Computer or a Network Client Computer, then the client computer is not allowed to connect to the TOE. Similarly, if the client computer presents an invalid or unknown (unrecognized CA) X.509v3 certificate, the IPsec mutual authentication mechanism will fail.

The TOE also uses IP addresses and X.509v3 certificates via the IKE protocols to connect to and identify other trusted IT products. See section 7.1.6.27 for more details.

The TOE supports the following versions of the IKE protocol:

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

Mutual identification and authentication must be completed before any tasks can be performed by a Network Client Computer or an Administrative Computer.

The service templates define the User Role of a client computer. The following service templates are used to define the TOE's User Roles for IPsec users:

- All Services (U.ADMINISTRATOR)
- Network Client Computers (U.NORMAL)

The All Services service template is provided with the TOE. The Network Client Computers service template is created by the administrator as part of the TOE's configuration guidance.

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 WS*), and SNMP interface.

IP address management is discussed in section 7.1.4.5. Certificate management is discussed in section 7.1.6.27.

This section maps to the following SFRs:

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

7.1.4 Data protection and access control

7.1.4.1 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. Only U.ADMINISTRATOR can create, modify, and delete Permission Sets. In addition, only U.ADMINISTRATOR can create, modify, and delete the Permission Set associations to users. By default, the TOE includes the following Permission Sets:

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

These default Permission Sets cannot be created, renamed or deleted. In addition, the permissions in Device Administrator cannot be modified.

Permissions in a Permission Set include permissions as high-level as executing the Retrieve from Device Memory application. They also include more granular permissions that control administrative functions like the ability to delete any 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

7.1.4.2 Job PINs

Users can control access to each stored print and stored copy job that they place under the TOE's control by assigning a Job PIN to each job. A Job PIN limits access to a stored print or stored copy job while the job resides under the TOE's control and allows a user to control when the job is printed so that physical access to the hard copies can be controlled by the user. 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. They cannot be assigned after the job already resides under the TOE's control. 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 at the client computer. The Job PIN is embedded in the print job by the client computer prior to sending the print job to the TOE. Once the TOE receives a print job containing a Job PIN, the TOE enforces the Job PIN embedded in that job.

Once a Job PIN is set on a job and the job resides under the TOE's control, the Job PIN cannot be modified or deleted (i.e., the TOE does not provide the ability to manage Job PINs).

A job with a Job Encryption Password cannot be assigned a Job PIN.

This section maps to the following SFRs:

- FIA_SOS.1

7.1.4.3 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 and AES-256 in CBC mode. 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. The decryption algorithm is included in the TOE. 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 or removed. In addition, a job with a Job Encryption Password cannot be assigned a Job PIN.

This section maps to the following SFRs:

- FCS_COP.1-job

7.1.4.4 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 a Job PIN or through the use of a Job Encryption Password. The user identifier for a stored 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 print 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 non-fax Job Storage jobs (D.DOC).

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 the TOE 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 TOE.

This section maps to the following SFRs:

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

7.1.4.5 TOE function access control

The TOE controls Control Panel access to TOE functions through the use of Permission Sets. The home screen sign-in process assigns the Permission Set to the authenticated user's session. This session Permission Set becomes the user's User Role. Access to each TOE device function is configurable in a Permission Set by an administrator. A user can perform any function permitted in the session Permission Set. Control Panel applications (e.g., Copy, Fax, Retrieve from Device Memory) use the user's Permission Set to determine which of the application's functions should be allowed or disallowed for the user. 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 the user's Permission Set.

Each Control Panel application requires the user to have one or more specific permissions in their session Permission Set in order to access that application. In addition, the TOE's administrator can map sign-in methods to each Control Panel application and require the user to be authenticated to that sign-in method in order to access that application. The individual applications only check and enforce permissions. They do not check the sign-in methods. Instead, the TOE enforces the sign-in method requirement at the time that the user signs in to the TOE by removing permissions from the user's session Permission Set for each application in which the user's sign in method does not match the sign in method required by the TOE. By removing the permissions required by each non-matching application, the TOE limits the set of applications that the user can access.

Administrators can change/modify the sign-in method mapped to each application. In addition, the TOE provides the feature “Allow users to choose alternate sign-in methods” which allows administrators to select if the sign-in method application mappings are enforced or ignored by the TOE. It is a function in the configuration settings which can be configured through the EWS (HTTP) or WS* web services. When this function is disabled, the TOE enforces the "sign-in method to application" mappings and prunes (reduces) the user's session Permission Set accordingly. When this function is enabled, the sign-in method mappings are ignored by the TOE and the user's session Permission Set remains unchanged.

For IPsec users, the TOE uses the IPsec/Firewall to control access to the supported network service protocols. The IPsec/Firewall contains the IP addresses of authorized client computers grouped into address templates and the network service protocols grouped into service templates. The administrator maps an address template to a service template using an IPsec/Firewall rule. Service templates, therefore, act as the User Roles for IPsec users. IP addresses of computers not contained in a rule are denied access to the TOE. 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

7.1.4.6 Residual information protection

When the TOE deletes an object defined in section 6.1.3.5, the contents of the object are no longer available to TOE users.

This section maps to the following SFR:

- FDP_RIP.1

7.1.5 Protection of the TSF

7.1.5.1 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 TOE 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 analog fax hardware and the firmware that controls the fax hardware do not have the ability to access the Shared-medium fax functions. No pathway is provided to the Shared-medium interface from the fax. The TOE's analog fax functions only support the sending and receiving of fax data. Fax commands with potential for accessing the Shared-medium interface are not supported by the TOE.

When the fax feature "Fax Archive" is enabled, the administrator can control the destination to which fax data is archived. The administrator can disable the fax feature "Fax Archive" to prevent data from being sent from the Public Switched Telephone Network (PSTN) to the local network.

This section maps to the following SFR:

- FMT_MOF.1-faxarchive
- FPT_FDI_EXP.1

7.1.5.2 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 have pre-requisites that must be met prior to execution in order to receive valid results. For example, the LDAP Settings verification test requires LDAP Sign In to be configured and enabled prior to executing the test. The tests that may be available during self-test include:

- Device User Access Code verification
- LDAP Settings verification
- Windows Setting verification

This section maps to the following SFR:

- FPT_TST.1

7.1.5.3 Reliable timestamps

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

This section maps to the following SFR:

- FPT_STM.1

7.1.6 TOE access protection

The following session termination mechanisms are supported by the TOE:

- Inactivity timeout
- Automatic logout

7.1.6.1 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 TOE. The inactivity period is managed by the administrator via EWS (HTTP) or WS* web services. Only one inactivity period setting exists per TOE.

This section maps to the following SFR:

- FTA_SSL.3

7.1.6.2 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

7.1.7 Trusted channel communication and certificate management

Shared-medium communications (i.e., Ethernet) between the TOE and other trusted IT products 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 mechanism(s) used to protect these channels and the channels protected by the mechanism(s).

Secure protocol	Network channel	Initiated by
IPsec	Email connections (SMTP gateway)	TOE
	EWS (HTTP) connections (including web browser & certificate upload)	Administrative Computer
	Windows domain controller (Kerberos) connections	TOE
	LDAP server connections	TOE
	PJL connections	Administrative Computer & Network Client Computer
	Save to Network Folder connections (SMB, FTP)	TOE
	Save to SharePoint connections (*flow* models only)	TOE
	SNMP connections	Administrative Computer

Secure protocol	Network channel	Initiated by
	Syslog server connections	TOE
	Web Services connections (OXPd & WS*)	Administrative Computer

Table 35: Trusted channel connections

The TOE uses 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 INSIDE Secure. The QuickSec cryptographic library is part of the Operational Environment, not the TOE. The TOE prepares the data and invokes the appropriate cryptographic functions, but the code in the QuickSec cryptographic library performs the processing and calculations required. INSIDE Secure performs regular and rigorous developer testing of the implementation of the cryptographic algorithms in the QuickSec cryptographic library.

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

- RSA 1024-bit and 2048-bit (Operational Environment)
- AES-128, AES-192, and AES-256 in CBC mode (Operational Environment)
- HMAC-SHA1-96 (Operational Environment)
- HMAC-SHA-256-128 (Operational Environment)
- HMAC-SHA-384-196 (Operational Environment)
- HMAC-SHA-512-256 (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 maintains X.509v3 certificates for IPsec in the certificate store:

- One network identity certificate
- One or more Certificate Authority (CA) certificates

The EWS (HTTP) and WS* Web Services allow administrators to manage these X.509v3 certificates used by IPsec. Additionally, OXPd Web Services can be used to manage the CA certificates used by IPsec.

When the TOE is first powered on, it generates a self-signed identity certificate to use for network identity. In the evaluated configuration, the use of a self-signed identity certificate generated by the TOE for network identity is not permitted. The administrator must import a CA-signed identity certificate and private key and designate this certificate for network identity usage. The TOE requires a network identity certificate to always exist; therefore, it allows the administrator to replace the network identity certificate used by IPsec.

The TOE uses a copy of the self-signed identity certificate it generates when first powered on as a CA certificate (self-signed) and comes with other CA certificates pre-installed. The administrator must obtain a CA certificate from the Operational Environment and install this certificate when setting up the evaluated configuration. The TOE allows the administrator to add, replace, and delete CA certificates used by IPsec.

This section maps to the following SFRs:

- FCS_CKM.1
- FCS_CKM.2
- FCS_COP.1-ipsec
- FMT_MTD.1-auth
- FMT_SMF.1
- FTP_ITC.1

7.1.8 User and access management

The TOE supports the following roles:

- Administrators (U.ADMINISTRATOR)
- Users (U.NORMAL)

Administrators maintain and configure the TOE and Operational Environment. Users perform the standard print, copy, fax, etc. functions on the system.

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 other trusted IT products to which the TOE will connect. Administrators do this by creating, modifying, and deleting IPsec/Firewall address templates, service templates, and rules via the TOE. Similarly, only administrators can create, modify, and delete address templates, service templates, and rules via the TOE for trusted IT products.

For each Control Panel application, an administrator can modify the association of a sign-in method to an application. (For example, the administrator can associate LDAP Sign In method to the Retrieve from Device Memory application). In addition, administrators control whether or not a Control Panel user must use the administrator-selected sign-in method associated with the applications in order to access that application. This latter feature is controlled through the "Allow users to choose alternate sign-in methods" function.

Administrators can initialize, modify, and delete Device User Accounts in the Local Device Sign In database.

It's worth noting that although the following security attributes are enforced by the TOE, the TOE does not provide functionality to manage these attributes (i.e., the TOE cannot add, change, delete, or query these attributes on an existing job) and the TOE does not provide default values for these attributes; therefore, there are no management SFRs specified in this ST for these security attributes:

- Job Encryption Password - The job is encrypted by the Operational Environment. The TOE does not provide a mechanism to change or delete the password on the job.
- Job PIN - A print job's Job PIN is set by the Operational Environment (i.e., Network Client Computer). The TOE does not provide a mechanism to change or delete a Job PIN from a print job.

This section maps to the following SFRs:

- FMT_MOF.1-auth
- 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)

ASCII

American Standard Code for Information Interchange

CA

Certificate Authority

CBC

Cipher Block Chaining

SMB

Server Message Block

DNS

Domain Name System

eMMC

embedded MMC

ESP

Encapsulating Security Payload (IPsec)

EWS

Embedded Web Server

HCD

Hardcopy Device

HMAC

Hashed Message Authentication Code

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 Printer

MMC

MultiMediaCard

NFC

Near Field Communication

NTLM

Microsoft NT LAN Manager

NTP

Network Time Protocol

OXP

Open Extensibility Platform

OXPd

OXP device layer

PIN

Personal Identification Number

PJL

Printer Job Language

PRF

Pseudo-random Function

PSTN

Public Switched Telephone Network

SFR

Security Functional Requirement

SHA

Secure Hash Algorithm

SMB

Server Message Block

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOAP

Simple Object Access Protocol

SSH

Secure Shell

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 the TOE.

Authentication Data

This includes the Access Code and/or password for each user of the product.

Control Panel Application

An application that resides in the firmware and is selectable by the user via the Control Panel.

Device Administrator Password

The password used to restrict access to administrative tasks via EWS, WS*, 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.

Near Field Communication (NFC)

Proximity (within a few inches) radio communication between two or more devices.

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.

Wireless Direct Print

Feature that enables Wi-Fi capable devices (for example: smart phones, tablets, or computers) to establish a direct peer-to-peer wireless connection with the printer to submit print jobs.

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 (CPY) 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 Document Fax (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 (PRT) 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 (SCN) 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 (SMI) 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) INSIDE Secure

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

RFC4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec

Author(s) S. Kelly, S. Frankel

Date 2007-05-01

Location http://www.ietf.org/rfc/rfc4868.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