HP Color LaserJet Enterprise MFP M776, HP LaserJet Enterprise MFP M634/M635/M636

Security Target

Version:	**1.2**
Status:	**Final**
Last Update:	**2021-07-01**
Classification:	**Public**

Trademarks

The following terms are trademarks of Hewlett-Packard Development Company, L.P. in the United States, other countries, or both.

- HP®
- LaserJet®

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

- 2600.1™
- 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®
- Authenticode®

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

- INSIDE Secure®
- QuickSec®

Other company, product, and service names may be trademarks or service marks of others.

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

Version	Date	Author(s)	Changes Made
1.2	2021-07-01	Gerardo Colunga & Anthony Peterson	Final version.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	**HP Color LaserJet Enterprise MFP M776,** **HP LaserJet Enterprise MFP M634/M635/M636** **Security Target**
Version:	1.2
Status:	Final
Date:	2021-07-01
Sponsor:	HP Inc.
Developer:	HP Inc.
Certification Body:	CSEC
Certification ID:	CSEC2019025
Keywords:	HP Inc., HP, LaserJet, Color LaserJet, hardcopy device, HCD, printer, MFP, M776, M634, M635, M636

1.2 TOE Identification

The TOE is the HP FutureSmart 4.10 Firmware for the HP Color LaserJet Enterprise MFP M776 and HP LaserJet Enterprise MFP M634/M635/M636 multifunction printers. The complete list of the TOE models along with the firmware versions for the models is provided in Table 1.

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 [PP2600.1] protection profile.

The TOE contains functions for copying, printing, faxing, scanning, storing, and retrieving of documents. These hardcopy devices (HCDs), as they are called in [PP2600.1], are self-contained units that include processors, memory, networking, one storage drive, 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 which are part of the Operational Environment.

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)
- Trusted channel communication and certificate management
- User and access management

1.4.1 Required and Optional Hardware, Software, and Firmware

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

- The applicable MFP model from Table 1 for running the TOE firmware.
- Domain Name System (DNS) server
- One administrative client computer connected to the TOE in the role of an Administrative Computer. It must contain:
    - Web browser
- One or both of the following:
    - Lightweight Directory Access Protocol (LDAP) server
    - Windows domain controller/Kerberos server
- Syslog server
- Windows Internet Name Service (WINS) server
- Network Time Protocol (NTP) server

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

- Client computers connected to the TOE in a non-administrative computer role
- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- Simple Mail Transfer Protocol (SMTP) gateway
- Microsoft SharePoint
- Remote file systems:
    - File Transfer Protocol (FTP)
    - Server Message Block (SMB)

1.4.2 Intended Method of Use

[PP2600.1] is defined for a commercial information processing environment in which a high 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 the storing and retrieving of 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 computers via a wired local area network using HP's embedded Jetdirect Inside print server 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 Embedded Web Server (EWS) interface and Representational State Transfer (REST) Web Services interface for managing the TOE over HTTP.

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

1.5 TOE Description

1.5.1 TOE Models and Firmware Versions

Table 1 shows the HCD models included in this evaluation.

Physically speaking, all models use the same ASIC and processor. All models contain one field-replaceable nonvolatile storage drive. All models have a Control Panel for operating the HCD locally and Ethernet network capability for connecting to a network. They all support submission of print jobs over the network and remote administration over the network. The main physical differences between models are floor models versus table top models, the number and size of paper feeders, the scan and print speed, the number of output bins, and whether they contain a stapler/stacker. Some models come with an analog fax modem included versus others where the modem is optional.

All TOE models use the same Jetdirect Inside firmware version.

- JSI24100002

The TOE includes the following System firmware versions

- 2410028_055041 (HP FutureSmart 4.10 Firmware)

- 2410028_055025 (HP FutureSmart 4.10 Firmware)

Table 1 includes lists the TOE models along with the product number for each model.

Table 1: TOE reference

Product model name	Product number	System firmware version
HP Color LaserJet Enterprise MFP M776dn	T3U55A	2410028_055041
HP Color LaserJet Enterprise Flow MFP M776z	3WT91A	2410028_055041
HP Color LaserJet Enterprise Flow MFP M776zs	T3U56A	2410028_055041
HP LaserJet Enterprise MFP M634dn	7PS94A	2410028_055025
HP LaserJet Enterprise Flow MFP M634h	7PS95A	2410028_055025
HP LaserJet Enterprise MFP M634z	7PS96A	2410028_055025
HP LaserJet Enterprise MFP M635fht	7PS98A	2410028_055025
HP LaserJet Enterprise MFP M635h	7PS97A	2410028_055025
HP LaserJet Enterprise Flow MFP M635z	7PS99A	2410028_055025
HP LaserJet Enterprise MFP M636fh	7PT00A	2410028_055025
HP LaserJet Enterprise Flow MFP M636z	7PT01A	2410028_055025

The following table lists the English-guidance documentation for the TOE:

Table 2: English-only guidance documentation

MFP models	Title	Reference
All	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP Color LaserJet Enterprise MFP M776, HP LaserJet Enterprise MFP M634/M635/M636 Edition 1, 4/2021	[CCECG]
M776dn, M776z, M776zs	HP Color LaserJet Enterprise MFP M776 User Guide Edition 1, 10/2019	[M776-UG]

MFP models	Title	Reference
M776dn, M776z	HP Color LaserJet Enterprise MFP M776dn, M776z M776dn M776z Installation Guide 2019	[M776DN_Z-IG]
M776zs	HP Color LaserJet Enterprise MFP M776zs M776zs Installation Guide 2019	[M776ZS-IG]
M634dn, M634h, M634z, M635h, M635fht, M635z, M636fh, M636z	HP LaserJet Enterprise MFP M634 HP LaserJet Enterprise MFP M635 HP LaserJet Enterprise MFP M636 User Guide Edition 1, 5/2020	[M634_5_6-UG]
M634dn, M634h, M634z, M635h, M635fht, M635z, M636fh, M636z	HP LaserJet Enterprise MFP M634 HP LaserJet Enterprise MFP M635 HP LaserJet Enterprise MFP M636 M634dn, M634h, M634z, M635h, M635fht, M635z, M636fh, M636z Installation Guide 2020	[M634_5_6-IG]

The firmware, [CCECG], and other supporting files are packaged in a single ZIP file (i.e., a file in ZIP archive file format). This ZIP file is available for download from the HP Inc. website. The firmware is packaged in this ZIP file as a single firmware bundle.

The consumer receives the hardware independent of the ZIP file. The evaluated hardware models, which are defined in Table 1, are either already on the consumer's premises or must be obtained from HP Inc.

1.5.2 TOE Architecture

As mentioned previously, the TOE is the firmware of an MFP designed to be shared by many client computers and human users. It performs the functions of printing, copying, scanning, faxing, storing, and retrieving of documents. The TOE can be connected to a wired local network through the embedded Jetdirect Inside print server'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

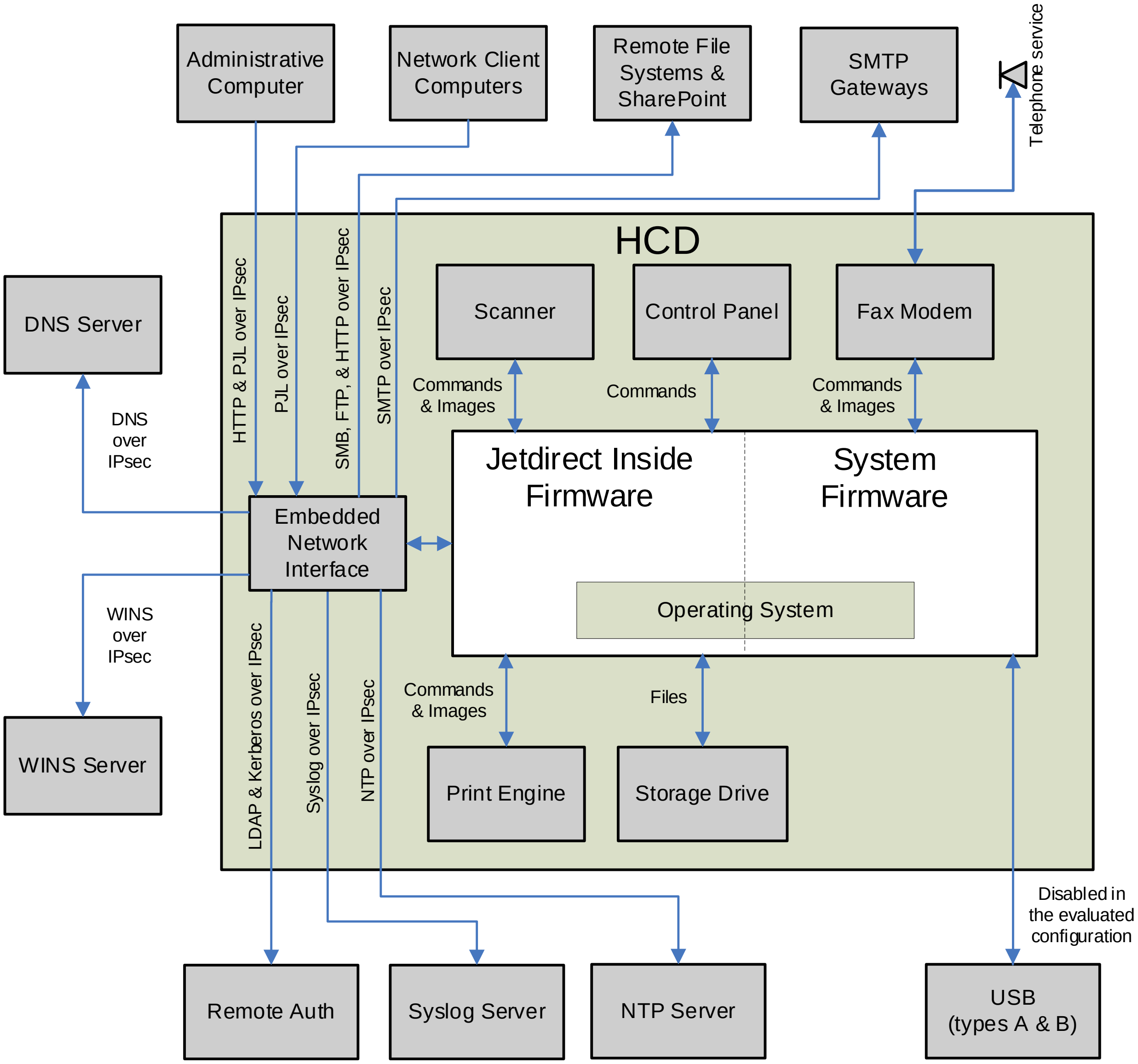


Figure 1 shows a high-level physical diagram of an HCD with the unshaded areas representing the TOE and the shaded areas indicating components that are part of the Operational Environment.

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)
- Representational State Transfer (REST) Web Services

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

The REST Web Services interface allow administrators to externally manage the TOE over HTTP.

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 networking port 9100 on the TOE.

The TOE protects all non-broadcast/non-multicast 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 along 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.

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.

The TOE protects stored non-fax jobs with either a 4-digit Job PIN or by accepting (and storing) an encrypted print 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, all stored non-fax jobs must either be assigned a 4-digit Job PIN or be an encrypted print job.

The TOE also supports Microsoft SharePoint 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 can encrypt stored document files according to the Adobe PDF specification.

The TOE can be used to email scanned documents. In addition, the 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 emails up to the SMTP gateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

The TOE supports name resolution using the DNS and WINS. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to the name resolution servers.

The TOE automatically synchronizes its system clock with an NTP server. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to the NTP server.

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 is 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 local and remote sign-in methods for I&A of users.

- Local sign-in method:
    - Local Device Sign In
- Remote sign-in methods:
    - LDAP Sign In
    - Windows Sign In

The Local Device Sign In method maintains the account information within the TOE. Only the Device Administrator account, which is an administrative account, is supported through this method in the evaluated configuration. 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 have field-replaceable nonvolatile storage drive (a.k.a. storage drive) that resides in the Operational Environment. The field-replaceable nonvolatile storage drive is a disk-based, self-encrypting hard disk drive.

The storage drive contains a section called Job Storage which is a user-visible filesystem where stored print, stored copy, and stored received faxes are stored/held. All jobs in Job Storage are automatically persisted across power cycles except Personal Jobs, which are a type of stored print job. Personal Jobs can be persisted across power cycles or deleted depending on how the administrator configures the TOE. (Job types are discussed in section 1.5.5.2.1)

The TOE supports the auditing of document-processing functions and security-relevant events 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.

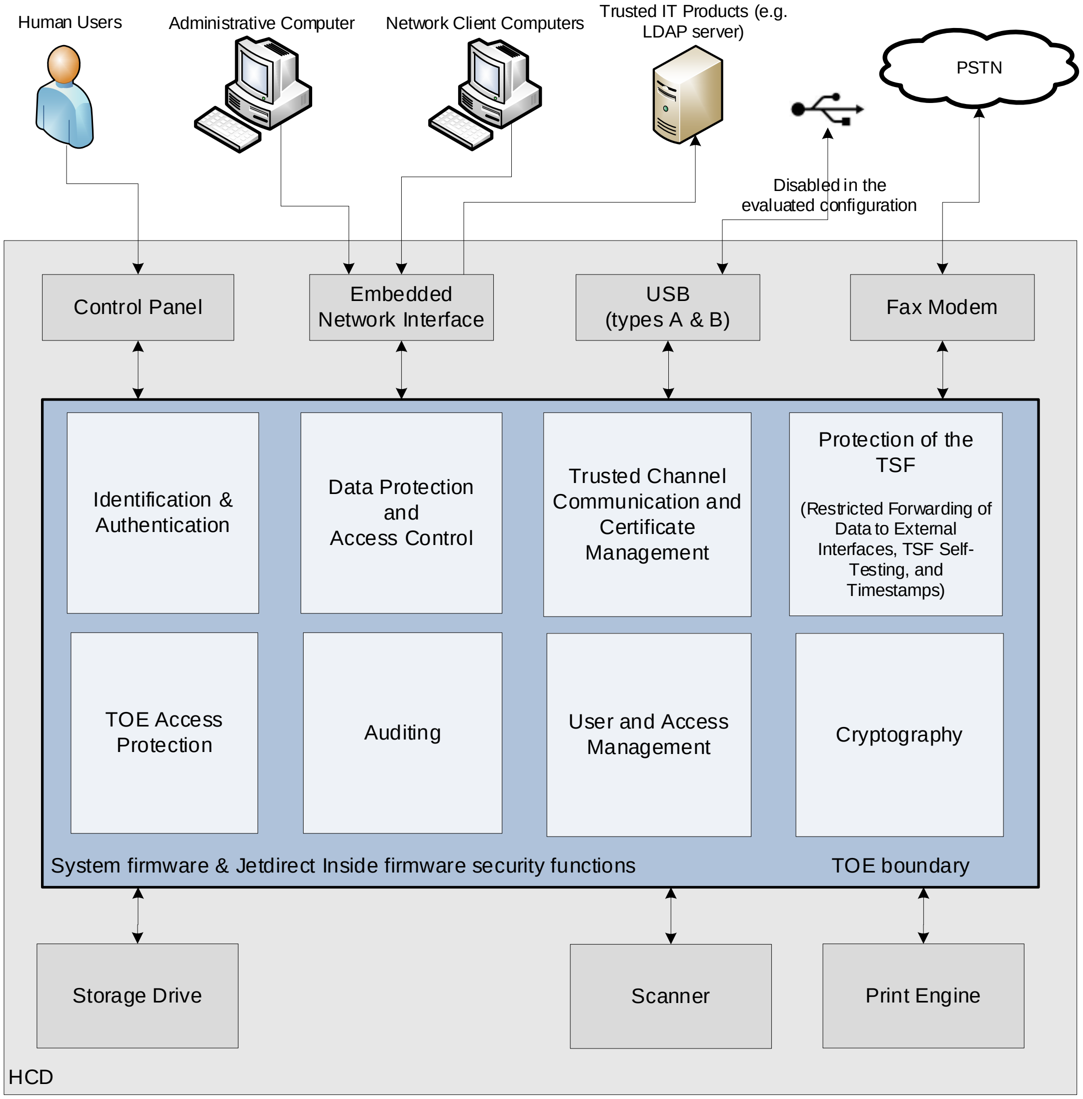
The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. They are shown as two separate components but they both share the same operating system (OS). The operating system is part of the Operational Environment. Both firmware components also contain an Embedded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

The Jetdirect Inside firmware includes 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 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 System firmware and the Jetdirect Inside firmware excluding the underlying operating system). The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the System firmware. The System firmware and Jetdirect Inside firmware share the same operating system (which is part of the Operational Environment). The 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 Scope Diagram


Human Users
Administrative Computer
Network Client Computers
Trusted IT Products (e.g. LDAP server)
PSTN
Disabled in the evaluated configuration
Control Panel
Embedded Network Interface
USB (types A & B)
Fax Modem
Identification & Authentication
Data Protection and Access Control
Trusted Channel Communication and Certificate Management
Protection of the TSF
(Restricted Forwarding of Data to External Interfaces, TSF Self-Testing, and Timestamps)
TOE Access Protection
Auditing
User and Access Management
Cryptography
System firmware & Jetdirect Inside firmware security functions
TOE boundary
Storage Drive
Scanner
Print Engine
HCD

1.5.3 TOE Security Functionality (TSF) Summary

1.5.3.1 Auditing

The TOE performs auditing of document-processing functions and security-relevant events. Both the Jetdirect Inside and 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.)

1.5.3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The HP FutureSmart QuickSec 5.1 (a.k.a. QuickSec) cryptographic library within the TOE is used to supply the cryptographic algorithms for IPsec. See section 1.5.3.7 for more information.

The TOE supports key derivation and decryption for printing encrypted stored print jobs. Both the key derivation function and decryption algorithm used by the TOE for printing encrypted stored print jobs are included in the TOE. See section 1.5.3.4.3 for more information.

The TOE contains a Data Integrity Test that provides administrators the ability to verify the integrity of specific TSF Data on-demand through the EWS. The Data Integrity Test uses the SHA-256 algorithm to verify the integrity of TSF Data. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA2-256 algorithm. See section 1.5.3.5.3 for more information.

The TOE contains a Code Integrity Test that provides administrators the ability to verify the integrity of TOE executable code files stored on the storage drive on-demand through the EWS. The Code Integrity Test uses the SHA-256 algorithm to verify the integrity of TOE executable code files. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA2-256 algorithm. See section 1.5.3.5.3 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.

1.5.3.2.1 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 [PP2600.1] requirements.

All MFP models contain a disk-based, self-encrypting storage drive. The self-encrypting storage drive provides hardware-based cryptography and persistent storage to securely manage sensitive document and system data. Data on a self-encrypting storage drive is encrypted and the encryption key is locked to the HCD. The cryptographic functionality is transparent to the TOE and to the user.

1.5.3.3 Identification and Authentication

1.5.3.3.1 Control Panel I&A

From the Control Panel, the user can perform the following actions prior to authentication.

- Viewing of help information
- Viewing of device status information
- Viewing of network connectivity status information
- Viewing of system time
- Viewing of Web Services status information
- Viewing of Welcome screen

- Selection of Sign In
- Selection of sign-in method from Sign In screen
- Printing of help information
- Printing of network connectivity status information
- Changing language for the session
- Resetting of session

The Control Panel user cannot perform any other TSF-mediated actions until after the user has been successfully identified and authenticated.

Users select the sign in method from a menu of sign in methods. The menu options vary depending on the number of remote sign-in methods configured for the TOE. The Control Panel supports the following local and remote sign-in methods in the evaluated configuration.

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)

Although the Local Device Sign In method supports multiple accounts, only the built-in Device Administrator account (U.ADMINISTRATOR) is to be used with this method in the evaluated configuration. The administrator must not create any Local Device Sign In accounts.

For successful authentication using a remote sign-in method, Control Panel users must enter their username and password as defined on the remote authentication server.

When users sign in through the Control Panel, the TOE displays dots for each character of access code or password typed to prevent onlookers from viewing another user's authentication data. The TOE also contains account lockout functionality for the built-in Device Administrator account to help prevent password discovery through a brute-force attack.

1.5.3.3.2 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 Rivest-Shamir-Adleman (RSA) X.509v3 certificates to authenticate the users. The IP address of a connecting client computer must be defined in the TOE's IPsec/Firewall 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 two 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). Table 3 shows the mapping of IPsec users to their allowed network protocols in the evaluated configuration.

Table 3: IPsec user mappings to allowed network protocols

IPsec user	Allowed network protocol access
Administrative Computer (U.ADMINISTRATOR)	EWS (HTTP), REST Web Services (HTTP) and PJL (TCP port 9100)
Network Client Computer (U.NORMAL)	PJL (TCP port 9100)

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 the EWS interface and REST Web Services interface 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. Both IKEv1 and IKEv2 are supported in the evaluated configuration.

In addition, the TOE can contact many types of trusted IT products using IPsec and mutual authentication. The TOE contacts these trusted IT products either to send data to them (e.g., send email alert to the SMTP gateway) or to request information from them (e.g., authenticate a user using LDAP). The TOE mutually authenticates these trusted IT products via IPsec prior to sending data or requesting information from them.

1.5.3.4 Data Protection and Access Control

1.5.3.4.1 Permission Sets

The TOE controls user access to functions available at the Control Panel using permissions. Each Control Panel application and protected feature has an associated permission. A permission is configured to either grant or deny access. Permissions are defined in Permission Sets (a.k.a. User Roles) which are assigned to users. To execute a Control Panel application or protected feature, the applicable permission must be configured to grant access in the Permission Set applied to a user. The Permission Set applied to a user is a combination of Permission Sets assigned to the user.

The TOE contains built-in Permission Sets. The built-in Permission Sets are:

- Device Guest
- Device Administrator

- Device User

Built-in Permission Sets cannot be deleted or renamed. Additionally, the permissions defined in the Device Administrator Permission Set cannot be configured (i.e. the permissions are always set to grant access). In addition to the built-in Permission Sets, the TOE provides the ability to add custom Permission Sets. Permission Sets are stored in the TOE and are managed via the EWS.

The following table lists the access control level each Permission Set provides, and the User Role each Permission Set is assigned to in the evaluated configuration.

Table 4: Permission sets to user roles

Permission set	Access control level	Assigned to user role
Device Guest	None (The Device Guest Permission Set has all permissions configured to deny access.)	All
Device Administrator	Administrative (The Device Administrator Permission Set has all permissions set to grant access. With all permissions set to grant access, the Device Administrator Permission Set provides access to all functions.)	U.ADMINISTRATOR
Device User	Non-administrative (The Device User Permission Set has all permissions for administrative functions configured to deny access.)	U.NORMAL
Custom (if any are added by U.ADMINISTRATOR)	Non-administrative (The Custom Permission Set has all permissions for administrative functions configured to deny access.)	U.NORMAL

1.5.3.4.2 Job PINs

Users control access to print (non-encrypted) 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.

1.5.3.4.3 Job Encryption Password

The TOE can store and decrypt encrypted stored print jobs received from a client computer that 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 print or delete an encrypted stored print job at the Control Panel, a non-administrative user must provide the correct Job Encryption Password for the encrypted stored print job. An administrative user can delete an encrypted stored print job at the Control Panel without providing a Job Encryption Password but must provide the correct Job Encryption Password to print the job.

1.5.3.4.4 Common Access Control

The TOE protects each non-fax job in Job Storage from non-administrative users using 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. 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.

1.5.3.4.5 TOE Function Access Control

For Control Panel users, the TOE controls access to Control Panel applications (e.g., Print from Job Storage) 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 into 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 at the product control panel." 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.

1.5.3.4.6 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.

1.5.3.5 Protection of the TSF

1.5.3.5.1 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. The TOE does not provide a pathway or support for commands necessary to achieve network access through the analog fax phone line connection.

1.5.3.5.2 TSF Self-Testing

The TOE contains a suite of self tests to test specific security functionality of the TOE. It contains an on-demand Data Integrity Test to verify the integrity of specific TSF Data of the TOE, and an on-demand Code Integrity Test to verify the integrity of TOE executable code files stored on the storage drive.

1.5.3.5.3 Reliable Timestamps

The TOE contains a system clock that is used to generate reliable timestamps. In the evaluated configuration, the TOE must be configured to synchronize its system clock with a Network Time Protocol (NTP) server.

1.5.3.6 TOE Access Protection

1.5.3.6.1 Inactivity Timeout

The Control Panel supports an Inactivity Timeout in case users forget to sign out of the Control Panel after signing in.

1.5.3.7 Trusted Channel Communication and Certificate Management

The TOE supports IPsec to protect data being transferred over the Shared-medium Interface. IPsec along with IKE use Diffie-Hellman (DH) key establishment (a.k.a. key exchange) to establish the key used for the secure channel, IP addresses and RSA X.509v3 certificates to identify and authenticate the endpoint, and the Advanced Encryption Standard (AES) with cipher block chaining (CBC) to protect the data transfers between the TOE and the endpoint using the key derived from the key establishment. DH uses the Digital Signature Algorithm (DSA) for key generation. In addition, the Secure Hash Algorithm (SHA) and Hashed Message Authentication Code (HMAC) based on SHA are used as part of the IPsec/IKE protocol. A deterministic random bit generator (DRBG)—specifically the counter DRBG CTR_DRBG(AES) that uses AES—is used to generate cryptographically random numbers for creating encryption keys, key material, and secret keys.

The IPsec and IKE cryptographic algorithms are all supplied by the QuickSec cryptographic library.

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

- RSA 2048-bit, and 3072-bit signature generation and verification
- DSA 2048-bit, 3072-bit, 4096-bit, 6144-bit, and 8192-bit key pair generation
- DH (IKEv1, IKEv2) key establishment/exchange
- AES-128, AES-192, and AES-256 in CBC mode for data transfers
- AES-256 (with ECB mode) for the CTR_DRBG(AES)
- CTR_DRBG(AES)
- SHA-1, SHA-256, SHA-384, and SHA-512 hashing
- HMAC-SHA1-96
- HMAC-SHA-256-128
- HMAC-SHA-384-192
- HMAC-SHA-512-256

In addition, the TOE provides certificate management functions used to manage X.509v3 certificates used for IPsec authentication.

1.5.3.8 User and Access Management

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

- Administrator (U.ADMINISTRATOR)

- Normal User (U.NORMAL)

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

1.5.4 TOE Boundaries

1.5.4.1 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 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 nonvolatile storage device from the perspective of [PP2600.1].

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.

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).

1.5.4.2 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)
- Trusted channel communication and certificate management
- User and access management

1.5.4.3 Evaluated Configuration

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

- Only one Administrative Computer is used to manage the TOE.
- Third-party solutions must not be installed on the TOE.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.DISALLOWED.
- OAUTH2 use is disallowed.
- SNMP over HTTP use is disallowed.
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password.
- HP Digital Sending Software (DSS) must be disabled.
- All received faxes must be converted into stored faxes.
- Fax Polling Receive must be disabled.
- Fax Archive must be disabled.
- Fax Forwarding must be disabled.
- Internet Fax and LAN Fax must be disabled.
- PC Fax Send must be disabled.
- Device USB and Host USB plug and play must be disabled.
- Control Panel Mandatory Sign-in must be enabled (this disables the Guest role).
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- User names for the LDAP and Windows Sign In users must only contain the characters defined in P.USERNAME.CHARACTER_SET.
- Local Device Sign In accounts must not be created (i.e., only the built-in Device Administrator account is allowed as a Local Device Sign In account).
- Device Administrator Password must be set as per P.ADMIN.PASSWORD.
- Remote Configuration Password must not be configured.
- PJL device access commands must be disabled.
- Firmware upgrades sent as print jobs through P9100 interface must be disabled.
- HP JetAdvantage Link Platform must be disabled.
- PJL drive access and PS drive access must be disabled.
- Wireless functionality must be disabled:
    - Near Field Communication (NFC) must be disabled.
    - Bluetooth Low Energy (BLE) must be disabled.

    - Wireless Direct Print must be disabled.
    - Wireless station must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- SNMP 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.
- Access must be blocked to the following Web Services (WS) using the Jetdirect Inside's IPsec/Firewall:
    - Open Extensibility Platform device (OXPd) Web Services
    - WS* Web Services

1.5.5 Security Policy Model

This section describes the security policy model for the TOE. Much of the terminology in this section comes from [PP2600.1] and is duplicated here so that readers won't have to read [PP2600.1] to understand the terminology used in the rest of this Security Target document.

1.5.5.1 Subjects/Users

Users are entities that are external to the TOE and which interact with the TOE. TOE users are defined in Table 5.

Table 5: TOE users

<table>
<tr><th>Designation</th><th colspan="2">Definition</th></tr>
<tr><td rowspan="4">U.USER</td><td colspan="2">Any authorized User. Authorized Users are U.ADMINISTRATOR and U.NORMAL.</td></tr>
<tr><th>Designation</th><th>Definition</th></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>U.ADMINNISTRATOR</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>

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 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 Computer -** Computer (U.ADMINISTRATOR entity) that can successfully authenticate to the TOE's administrative interface (e.g., EWS (HTTP) and REST Web Services (HTTP)) 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).

1.5.5.2 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

1.5.5.2.1 User Data

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

- User Document Data
- User Function Data

Table 6: User data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in hardcopy or electronic form, image data, or residually-stored data created by the 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.

User Data objects include:

- **Fax jobs**:
  - **Fax Receive jobs -** Fax jobs received by the TOE over the analog fax phone line where the connection is initiated by another fax device.
  - **Fax Send jobs -** Fax jobs being sent by the TOE over the analog fax phone line. (The Fax Send 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 depending on how the administrator configures the TOE. In the evaluated configuration, these jobs are automatically deleted after an administrator-specified time interval.
  - **Stored jobs -** Print jobs such as a personnel form, time sheet, or calendar from a client computer that are stored 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.
  - **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.
- **Scan job types**:

  - **Email jobs -** Scan jobs that are scanned directly into an email and sent from the TOE to an SMTP gateway.
  - **Scan to Network Folder jobs -** Scan jobs that are saved to a remote file system.
  - **Scan 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.

1.5.5.2.2 TSF Data

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

Table 7: TSF data

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

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

Table 8: TSF data listing

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 PINs associated with PIN-protected stored print and PIN-protected stored copy jobs	X	
Content encryption keys associated with encrypted stored print jobs	X	

TSF data	D.CONF	D.PROT
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	

1.5.5.3 SFR Package Functions

Functions perform processing, storage, and transmission of data. The following [PP2600.1]-defined functions apply to this Security Target.

Table 9: SFR package functions

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

1.5.5.4 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 [PP2600.1]-defined attributes apply to this Security Target.

Table 10: SFR package attributes

Designation	Definition
+CPY	Indicates data that is associated with a copy job.
+DSR	Indicates data that is associated with a document storage and retrieval job.
+FAXIN	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.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL3, augmented by ALC_FLR.2.

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

- [PP2600.1]: IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A". Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-CPY]: SFR Package for Hardcopy Device Copy Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-DSR]: SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-FAX]: SFR Package for Hardcopy Device Fax Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-PRT]: SFR Package for Hardcopy Device Print Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-SCN]: SFR Package for Hardcopy Device Scan Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-SMI]: SFR Package for Hardcopy Device Shared-medium Interface Functions. Version 1.0 as of June 2009; demonstrable conformance.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

2.1 Protection Profile Tailoring and Additions

2.1.1 IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A" ([PP2600.1])

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 [PP2600.1]. Because no removable nonvolatile storage devices exist in the HCDs, this Security Target does not claim conformance to "2600.1-NVS SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A" contained in [PP2600.1].

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 [PP2600.1]. The term "n/a" means "not applicable". The term "common" is used to refer to that portion of [PP2600.1] to which all TOEs must conform (i.e., the portions not labeled as packages).

Table 11: SFR mappings between 2600.1 and the ST

[PP2600.1] 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 [PP2600.1] and FAU_GEN.1 from the [PP2600.1] 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 [PP2600.1] and the FDP_ACC.1's from the [PP2600.1] 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 [PP2600.1] and the FDP_ACF.1's from the [PP2600.1] packages claimed by the ST. The iteration name was changed from "(a)" to "-cac" (Common Access Control) for better understandability when reading the ST.

[PP2600.1] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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 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			FMT_MSA.1(a) was omitted because management of all security attributes can be covered by FMT_MSA.1.
FMT_MSA.1(b)	FMT_MSA.1			FMT_MSA.1(b) was omitted because management of all security attributes can be covered by FMT_MSA.1.

[PP2600.1] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
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			Iteration was omitted because only TSF Data that is not associated with a Normal User can be managed.
FMT_MTD.1.1(b)	None			Iteration was omitted because only TSF Data that is not associated with a Normal User can be managed.
FMT_SMF.1	FMT_SMF.1			n/a
FMT_SMR.1	FMT_SMR.1			n/a
FPT_STM.1	FPT_STM.1			Because the TOE can be configured to use NTP along with its internal time source, both A.SERVICES.RELIABLE and OE.SERVICES.RELIABLE apply.
FPT_TST.1	FPT_TST.1			n/a
FTA_SSL.3	FTA_SSL.3			n/a

These SFRs in the Security Target are not required by and do not map to the protection profile [PP2600.1].

Table 12: SFR mappings of non-PP2600.1 SFRs and the ST
(in the ST, but not required by or hierarchical to SFRs in PP2600.1)

[PP2600.1] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
None	FCS_CKM.1-ipsec	X		FCS_CKM.1-ipsec specifies the type of cryptographic keys generated for IPsec key establishment.
None	FCS_CKM.1-job	X		FCS_CKM.1-job specifies key derivation function used by the TOE to unlock an encrypted stored print job.
None	FCS_CKM.2			FCS_CKM.2 specifies cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec.
None	FCS_COP.1-ipsec	X		FCS_COP.1-ipsec specifies RSA signature generation and verification along with AES and HMAC cryptographic algorithms used by the TOE in IPsec.
None	FCS_COP.1-job	X		FCS_COP.1-job specifies the SHA and HMAC cryptographic algorithms used by the TOE to unlock encrypted stored print jobs and the AES decryption cryptographic algorithm used by the TOE for decrypting encrypted stored print jobs.
None	FCS_COP.1-tst	X		FCS_COP.1-tst specifies SHA cryptographic algorithms used by TSF self-testing.

[PP2600.1] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
None	FIA_AFL.1			The TOE locks the Device Administrator account (a.k.a. Local Administrator account) after an administrator configurable positive integer of unsuccessful Control Panel authentication attempts via the Local Device Sign In method. Recommended by [PP2600.1] APPLICATION NOTE 38.
None	FIA_SOS.1			FIA_SOS.1 specifies the Job PIN strength of certain authorization mechanisms used by the TOE.
None	FIA_UAU.7			The TOE masks Job PINs, Access Codes, and passwords. Recommended by [PP2600.1] APPLICATION NOTE 38.
None	FMT_MOF.1	X		The TOE allows administrators to manage the security functions Control Panel authorization, Windows Sign In, LDAP Sign In, account lockout for Local Administrator account, Inactivity Timeout for Control Panel user sign-in sessions, enhanced security event logging, and IPsec.
None	FCS_RBG_EXT.1			FCS_RBG_EXT.1 specifies the random bit generation used by IPsec.

2.1.2 SFR Package for Hardcopy Device Copy Functions ([PP2600.1-CPY])

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

Table 13: SFR mappings between 2600.1-CPY and the ST

[PP2600.1] 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).

2.1.3 SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions ([PP2600.1-DSR])

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

Table 14: SFR mappings between 2600.1-DSR and the ST

[PP2600.1] 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).

2.1.4 SFR Package for Hardcopy Device Fax Functions ([PP2600.1-FAX)]

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

Table 15: SFR mappings between 2600.1-DSR and the ST

[PP2600.1] 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).

2.1.5 SFR Package for Hardcopy Device Print Functions ([PP2600.1-PRT])

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

Table 16: SFR mappings between 2600.1-PRT and the ST

[PP2600.1] 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).

2.1.6 SFR Package for Hardcopy Device Scan Functions ([PP2600.1-SCN])

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

Table 17: SFR mappings between 2600.1-PRT and the ST

[PP2600.1] 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).

2.1.7 SFR Package for Hardcopy Device Shared-medium Interface Functions ([PP2600.1-SMI])

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

Table 18: SFR mappings between 2600.1-SMI and the ST

[PP2600.1] 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 [PP2600.1] and FAU_GEN.1 from the [PP2600.1] SMI SFR package.
FPT_FDI_EXP.1	FPT_FDI_EXP.1			n/a

[PP2600.1] SFR	Maps to ST SFR(s)	Iteration	Hierarchical substitution	Rationale
FTP_ITC.1	FTP_ITC.1			n/a

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

Table 19: Threats countered by the TOE

Threat	Description
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.

Threat	Description
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

Table 20: Physical assumptions

Assumption	Description
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

Table 21: Personnel assumptions

Assumption	Description
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. The organization security policies and procedures include security awareness training covering topics such as how to identify and avoid clicking on malicious links.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

3.3.1.3 Connectivity

Table 22: Connectivity assumptions

Assumption	Description
A.SERVICES.RELIABLE	When the TOE uses any of the network services DNS, Kerberos, LDAP, NTP, SMTP, syslog, SMB, SharePoint, and/or WINS, these services provide reliable information and responses to the TOE.
A.EMAILS.PROTECTED	For emails received by the SMTP gateway from the TOE, the transmission of emails between the SMTP gateway and the email’s destination is protected.

3.4 Organizational Security Policies

3.4.1 Included in the PP2600.1 Protection Profile

Table 23: Organizational security policies in the PP2600.1 protection profile

Organizational security policy	Description
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 PP2600.1 Protection Profile

Table 24: Organizational security policies in addition to the PP2600.1 protection profile

Organizational security policy	Description
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 the EWS (HTTP), REST Web Services (HTTP), and at the Control Panel.

Organizational security policy	Description
P.USERNAME.CHARACTER_SET	To prevent ambiguous user names in the TOE's audit trail, the user names of the LDAP and Windows Sign In 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

Table 25: Security objectives for the TOE

Security objective	Description
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

Table 26: Security objectives for the operational environment

Security objective	Description
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.

Security objective	Description
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. The organization security policies and procedures include security awareness training covering topics such as how to identify and avoid clicking on malicious links.
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 DNS, Kerberos, LDAP, NTP, SMTP, syslog, SMB, SharePoint, and/or WINS, these services shall provide reliable information and responses to the TOE.
OE.EMAILS.PROTECTED	The IT environment shall protect the transmission of emails from the SMTP gateway to the email’s destination.

Security objective	Description
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 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.

Table 27: Mapping of security objectives to threats and policies

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

Objective	Threats/OSPs
O.USER.AUTHORIZED	T.DOC.DIS T.DOC.ALT T.FUNC.ALT T.PROT.ALT T.CONF.DIS T.CONF.ALT P.USER.AUTHORIZATION

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.

Table 28: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

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
OE.PHYSICAL.MANAGED	A.ACCESS.MANAGED
OE.SERVICES.RELIABLE	A.SERVICES.RELIABLE
OE.EMAILS.PROTECTED	A.EMAILS.PROTECTED
OE.USER.AUTHORIZED	T.DOC.DIS T.DOC.ALT T.FUNC.ALT T.PROT.ALT T.CONF.DIS T.CONF.ALT P.USER.AUTHORIZATION

Objective	Assumptions/Threats/OSPs
OE.USER.PC.POLICY	A.USER.PC.POLICY
OE.USER.TRAINED	A.USER.TRAINING
OE.USERNAME.CHARACTER_SET	P.USERNAME.CHARACTER_SET

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:

Table 29: Sufficiency of objectives countering threats

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

Threat	Rationale for security objectives
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 appropriately grant authorization.

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:

Table 30: Sufficiency of objectives holding assumptions

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 Owner to provide appropriate User training.

Assumption	Rationale for security objectives
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. The organization security policies and procedures include security awareness training covering topics such as how to identify and avoid clicking on malicious links. 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 DNS, Kerberos, LDAP, NTP SMTP, syslog, SMB, SharePoint, 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 DNS, Kerberos, LDAP, NTP, SMTP, syslog, SMB, SharePoint, and/or WINS, establishes that these services provide reliable information and responses to the TOE.

Assumption	Rationale for security objectives
A.EMAILS.PROTECTED	The assumption: • For emails received by the SMTP gateway from the TOE, the transmission of emails between the SMTP gateway and the email's destination is protected. is upheld by: • OE.EMAILS.PROTECTED which protects the transmission of emails from the SMTP gateway to the email's destination

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:

Table 31: Sufficiency of objectives enforcing Organizational Security Policies

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

OSP	Rationale for security objectives
P.AUDIT.LOGGING	The OSP: - To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel. is enforced by: - O.AUDIT.LOGGED which creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration. - OE.AUDIT_STORAGE.PROTECTED which protects exported audit records from unauthorized access, deletion and modifications. - OE.AUDIT_ACCESS.AUTHORIZED which establishes responsibility of the TOE Owner to provide appropriate access to exported audit records. - OE.AUDIT.REVIEWED which establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	The OSP: - To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment. is enforced by: - O.INTERFACE.MANAGED which manages the operation of external interfaces in accordance with security policies. - OE.INTERFACE.MANAGED which establishes a protected environment for TOE external interfaces.

OSP	Rationale for security objectives
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), REST Web Services (HTTP) 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 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 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.

5 Extended Components Definition

This section contains the extended component definition(s) used by this ST.

5.1 Class FPT: Protection of the TSF

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:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
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**].

5.2 Class FCS: Cryptographic Support

5.2.1 Cryptographic Operation (Random Bit Generation) (FCS_RBG)

Family behaviour

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

There are no management activities foreseen.

Audit: FCS_RBG_EXT.1

There are no audit events foreseen.

5.2.1.1 FCS_RBG_EXT.1 – Random Bit Generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with NIST SP 800-90A using [selection: **Hash_DRBG(any), HMAC_DRBG(any), CTR_DRBG(AES)**].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by an entropy source that accumulates entropy from software-based noise sources with a minimum of [selection: **128 bits, 256 bits**] of entropy at least equal to the greatest security strength, according to NIST SP 800-57, of the keys and hashes that it will generate.
Rationale	Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation. This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

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.).

Table 32: Security functional requirements for the TOE

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		PP2600.1	No	No	Yes	Yes
	FAU_GEN.2 User identity association		PP2600.1	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1-ipsec Cryptographic key generation	FCS_CKM.1	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.1-job Cryptographic key generation	FCS_CKM.1	CC Part 2	Yes	No	Yes	No
	FCS_CKM.2 Cryptographic key establishment		CC part 2	No	Yes	Yes	No
	FCS_COP.1-ipsec Cryptographic operation for IPsec	FCS_COP.1	CC part 2	Yes	No	Yes	No
	FCS_COP.1-job Cryptographic operation for encrypted stored print jobs	FCS_COP.1	CC part 2	Yes	No	Yes	No
	FCS_COP.1-tst Cryptographic operation for TSF self-testing	FCS_COP.1	CC part 2	Yes	No	Yes	No
	FCS_RBG_EXT.1 Random Bit Generation		ECD	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FDP - User data protection	FDP_ACC.1-cac Common access control SFP	FDP_ACC.1	PP2600.1	Yes	No	Yes	No
	FDP_ACC.1-tfac TOE function access control SFP	FDP_ACC.1	PP2600.1	Yes	No	Yes	No
	FDP_ACF.1-cac Common access control functions	FDP_ACF.1	PP2600.1	Yes	No	Yes	No
	FDP_ACF.1-tfac TOE function access control functions	FDP_ACF.1	PP2600.1	Yes	No	Yes	No
	FDP_RIP.1 Subset residual information protection		PP2600.1	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		PP2600.1	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		PP2600.1	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

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FIA_UID.1 Timing of Control Panel identification		PP2600.1	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		PP2600.1	No	Yes	Yes	No
FMT - Security management	FMT_MOF.1 Management of authentication security functions behavior	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1 Management of security attributes	FMT_MSA.1	PP2600.1	Yes	No	Yes	Yes
	FMT_MTD.1 Management of TSF data	FMT_MTD.1	PP2600.1	Yes	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		PP2600.1	No	No	Yes	No
	FMT_SMR.1 Security roles		PP2600.1	No	No	Yes	No
FPT - Protection of the TSF	FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces		PP2600.1-SMI	No	No	Yes	No
	FPT_STM.1 Reliable time stamps		PP2600.1	No	No	No	No
	FPT_TST.1 TSF testing		PP2600.1	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FTA - TOE access	FTA_SSL.3 Control Panel TSF-initiated termination		PP2600.1	No	Yes	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		PP2600.1-SMI	No	Yes	Yes	Yes

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 33; 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 33 (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required); none.**

Table 33: Auditable events

Auditable event	Relevant SFR(s)	Audit Level	Additional information	[PP2600.1]
Job completion	FDP_ACF.1-tfac	Not specified	Type of job	Yes: Common
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

Auditable event	Relevant SFR(s)	Audit Level	Additional information	[PP2600.1]
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

6.1.1.2 User identity association (FAU_GEN.2)

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

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1-ipsec)

FCS_CKM.1.1 The TSF shall generate *asymmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in Table 34** and specified cryptographic key sizes **defined in Table 34** that meet the following: **the standards defined in Table 34**.

Table 34: Asymmetric cryptographic key generation

Protocol	Key generation algorithm	Key sizes	Standards
IPsec	DSA	2048-bit, 3072-bit, 4096-bit, 6144-bit, 8192-bit	[FIPS186-4] Finite Field Cryptography (FFC) “Digital Signature Standard (DSS)”

Application Note: *Random bit generation for FCS_CKM.1-ipsec is implemented by FCS_RBG_EXT.1.*

Application Note: *The asymmetric keys generated by the DSA algorithm are used by the key establishment algorithms specified in FCS_CKM.2.*

6.1.2.2 Cryptographic key generation (FCS_CKM.1-job)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specific cryptographic key generation algorithm **Password-Based Key Derivation Function 2 (PBKDF2) with HMAC-SHA-256** and specified cryptographic key sizes **256 bit** that meet the following: [**PKCS5v2.1**]

Application Note: *PBKDF2 is used to derive a key from a Job Encryption Password to unlock an encrypted stored print job.*

6.1.2.3 Cryptographic key establishment (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall *perform cryptographic key establishment* ~~distribute cryptographic keys~~ in accordance with a specified cryptographic key *establishment* ~~distribution~~ method **defined in Table 35** that meets the following: **the standards defined in Table 35**.

Table 35: Cryptographic key establishment

Protocol	Key establishment method	Standards
IPsec	IKEv1 (DH)	[RFC4109] Algorithms for Internet Key Exchange version 1 (IKEv1) [RFC4894] Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
	IKEv2 (DH)	[RFC4306] Diffie-Hellman key agreement method defined for the IKEv2 protocol; [RFC4718] IKEv2 Clarifications and Implementation Guidelines [RFC4894] Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec

6.1.2.4 Cryptographic operation for IPsec (FCS_COP.1-ipsec)

FCS_COP.1.1 The TSF shall perform **the operations defined in Table 36** in accordance with a specified cryptographic algorithm **defined in Table 36** and cryptographic key sizes **defined in Table 36** that meet the following: **the standards defined in Table 36**.

Table 36: Cryptographic operations for IPsec

Protocol	Operations	Algorithm	Key sizes (in bits)	Standards
IPsec	Signature generation and verification	RSA	2048, 3072	[PKCS1v1.5] Public-Key Cryptography Standard (PKCS) #1 v1.5: RSA Encryption Standard
	Symmetric encryption and decryption	AES	CBC: 128, 192, 256; ECB: 256	[FIPS197] Advanced Encryption Standard; [SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques
	Secure hash	SHA-1, SHA-256, SHA-384, SHA-512		[FIPS180-4] Secure Hash Standard (SHS); [RFC4894] Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
	Data authentication	HMAC-SHA1-96	160	[RFC2104] HMAC: Keyed-Hashing for Message Authentication; [RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH
		HMAC-SHA-256-128	256	[RFC2104] HMAC: Keyed-Hashing for Message Authentication; [RFC4868] Using HMAC-SHA-256-, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
		HMAC-SHA-384-192	384	
		HMAC-SHA-512-256	512	

6.1.2.5 Cryptographic operation for encrypted stored print jobs (FCS_COP.1-job)

FCS_COP.1.1 The TSF shall perform **the operations defined in Table 37** in accordance with a specified cryptographic algorithm **defined in Table 37** and cryptographic key sizes **defined in Table 37** that meet the following: **the standards defined in Table 37**.

Table 37: Cryptographic operations for encrypted stored print jobs

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
	Secure hash	SHA-256		[FIPS180-4] Secure Hash Standard (SHS)
	HMAC calculation	HMAC-SHA-256	256	[RFC2104] HMAC: Keyed-Hashing for Message Authentication

6.1.2.6 Cryptographic operation for TSF self-testing (FCS_COP.1-tst)

FCS_COP.1.1 The *HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) in the operational environment* ~~TSF~~ shall perform **the operations defined in Table 38** in accordance with a specified cryptographic algorithm **defined in Table 38** and cryptographic key sizes **defined in Table 38** that meet the following: **the standards defined in Table 38**.

Table 38: Cryptographic operations for TSF self-testing

Protocol	Operations	Algorithm	Key sizes (in bits)	Standards
TSF self-testing	Secure hash	SHA-256		[FIPS180-4] Secure Hash Standard (SHS)

6.1.2.7 Random Bit Generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with NIST SP 800-90A using **CTR_DRBG(AES)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from software-based noise sources with a minimum of **256 bits** of entropy at least equal to the greatest security strength, according to NIST SP 800-57, of the keys and hashes that it will generate.

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 39 on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 39**.

Table 39: Common Access Control SFP

Object	Operations(s)	Subject	Access control rules	[PP2600.1] 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. 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 Fax Receive 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.	Common
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,	Common

Object	Operations(s)	Subject	Access control rules	[PP2600.1] section
			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 Fax Receive 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.)	

Object	Operations(s)	Subject	Access control rules	[PP2600.1] section
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 Fax Receive 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+FAXOUT) Fax Send jobs cannot be read by any subject.	DSR, FAX

Object	Operations(s)	Subject	Access control rules	[PP2600.1] section
D.DOC+CPY	Read, Modify	U.NORMAL	There are no access control restrictions for read and modify access.	CPY

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 39** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 39, and for each, the indicated security attributes in Table 39.**

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 39 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 at the product control panel" 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, none**.

6.1.4 Identification and authentication (FIA)

6.1.4.1 Local Device sign in authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 3 to 10** unsuccessful authentication attempts occur related to **the last successful authentication for the indicated user identity for the following interfaces**

- **Control Panel**
    - **Local Device Sign In**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **lock the account**.

Application Note: *Multiple unsuccessful authentication attempts using the same authentication data are counted as just one unsuccessful authentication attempt by the 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:**
  - **Local Device Sign In (Local Administrator account only)**
    - **User Identifier: Display name**
    - **User Role: Permission set**
  - **Windows Sign In**
    - **User Role: Permission set**
  - **LDAP Sign In**
    - **User Role: Permission set**
- **IPsec users:**
  - **User Identifier: IP address**
  - **User Role: 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 help information**
- **Viewing of device status information**
- **Viewing of network connectivity status information**
- **Viewing of system time**
- **Viewing of Web Services status information**
- **Viewing of Welcome screen**
- **Selection of Sign In**

- **Selection of sign-in method from Sign In screen**
- **Printing of help information**
- **Printing of network connectivity status information**
- **Changing language for the session**
- **Resetting of session**

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 *dots ("●")* to users while the *Control Panel* authentication is in progress.

Application Note: *Job PINs and Job Encryption Passwords are not used for authentication, but the digits are masked within dots ("●") when entered.*

6.1.4.7 Timing of Control Panel identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

- **Viewing of help information**
- **Viewing of device status information**
- **Viewing of network connectivity status information**
- **Viewing of system time**
- **Viewing of Web Services status information**
- **Viewing of Welcome screen**
- **Selection of Sign In**
- **Selection of sign-in method from Sign In screen**
- **Printing of help information**
- **Printing of network connectivity status information**
- **Changing language for the session**
- **Resetting of session**

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:

1. **User Identifier**
    - **Control Panel users:**
        - **Local Device Sign In: Display name**
        - **Windows Sign In: Windows username**
        - **LDAP Sign In: LDAP username**
    - **IPsec users:**
        - **IP address**
2. **User Role**
    - **Control Panel users:**
        - **Local Device Sign In: Permission set**
        - **Windows Sign In: Permission set**
        - **LDAP Sign In: Permission set**
    - **IPsec users:**
        - **IPsec/Firewall service template**

Application Note: *Incoming analog fax phone line users have no security attributes, but Fax Receive 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 at the product control panel" is disabled, the Control Panel 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 security functions (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to **perform the actions defined in** Table 40 **on** the functions **defined in Table 40** to **U.ADMINISTRATOR**.

Table 40: Management of functions

Function(s)	**Action(s)**	**Application note**
Control Panel user authorization	determine the behavior of, modify the behavior of	The “Allow users to choose alternate sign-in methods at the product control panel” function affects how the TOE authorizes control panel users. When this function is disabled, the sign-in method to application mappings are enforced during control panel user authorization.
Windows Sign In	disable, enable, determine the behavior of, modify the behavior of	In the evaluated configuration, at least one external authentication mechanism must be enabled.
LDAP Sign In	disable, enable, determine the behavior of, modify the behavior of	In the evaluated configuration, at least one external authentication mechanism must be enabled.
Account lockout for Local Administrator account	disable, enable, determine the behavior of, modify the behavior of	In the evaluated configuration, account lockout for the Local Administrator account must be enabled.
Inactivity Timeout for Control Panel user sign-in sessions	determine the behavior of, modify the behavior of	In the evaluated configuration, the Control Panel Inactivity Timeout must be set to value in the range of 10-60 seconds.
Enhanced security event logging	disable, enable	In the evaluated configuration, enhanced security event logging must be enabled.

Function(s)	Action(s)	Application note
IPsec	disable, enable, determine the behavior of, modify the behavior of	In the evaluated configuration, IPsec must be enabled.

6.1.5.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the **Common Access Control SFP in** Table 41 **and TOE Function Access Control SFP** to restrict the ability to **perform the operations defined in Table 41 on** the security attributes **defined in Table 41** to **U.ADMINISTRATOR**.

Table 41: Management of security attributes

Security attributes(s)	Operation(s)	Application note
User Identifier		
Custom IPsec/Firewall address template	query, create, modify, delete	The TOE provides the capability to create custom IPsec/Firewall address templates. A custom IPsec/Firewall address template defines two or more IP addresses for which the address template is to apply.
Role		
Built-in Device Administrator permission set	query	The TOE contains a built-in Device Administrator permission set that cannot be renamed or deleted. In the evaluated configuration, U.ADMINISRATOR users must be granted the Device Administrator permission set.
Built-in Device User permission set	query	The TOE contains a built-in Device User permission set that cannot be renamed or deleted. In the evaluated configuration, U.NORMAL users must be granted either the built-in Device User permission set or a custom permission set (if any exist).

Security attributes(s)		Operation(s)	Application note
	Custom permission set	query, create, modify, delete	The TOE provides the capability to create custom permission sets. A custom permission set can be renamed or deleted. In the evaluated configuration, U.NORMAL users must be granted either the built-in Device User permission set or a custom permission set (if any exist).
	Permissions associated with built-in Device Administrator permission set	query	The built-in Device Administrator permission set has all permissions enabled. The permissions associated with the Device Administrator permission set cannot be disabled.
	Permissions associated with built-in Device User permission set	query, enable, disable	The permissions associated with the built-in Device User permission set can be enabled or disabled. In the evaluated configuration, the built-in Device User permission set must have all administrative permissions disabled.
	Permissions associated with a custom permission set	query, enable, disable	The permissions associated with a custom permission set can be enabled or disabled. In the evaluated configuration, any custom permission sets created must have all administrative permissions disabled.
	Built-in IPsec/Firewall All Services template	query	The TOE contains a built-in IPsec/Firewall All Services template. The built-in IPsec/Firewall All Services template cannot be renamed or deleted. In the evaluated configuration, built-in IPsec/Firewall All Services template must be granted to the Administrative Computer (U.ADMINISTRATOR).
	Custom IPsec/Firewall service template	query, create,	The TOE provides the capability to create custom IPsec/Firewall service templates.

Security attributes(s)		Operation(s)	Application note
		delete, modify	In the evaluated configuration, two custom IPsec/Firewall service templates must be created: One custom IPsec/Firewall service template for Network Client Computers (U.NORMAL). One custom IPsec/Firewall service template for trusted IT products.
	Network services associated with built-in IPsec/Firewall All Services template	query	The built-in IPsec/Firewall All Services template has all network services enabled. Network services associated with the built-in IPsec/Firewall All Services template cannot be disabled.
	Network services associated with a custom IPsec/Firewall services template	query, enable, disable	Network services associated with a custom IPsec/Firewall services template can be enabled or disabled. In the evaluated configuration; The custom IPsec/Firewall service template for Network Client Computers (U.NORMAL) must only have the P9100 services enabled. The custom IPsec/Firewall service template for trusted IT products must only have those network services (e.g. SMTP) required for the TOE to establish an IPsec connection with the trusted IT products to either send data to them or request data from them. The custom IPsec/Firewall service template must not contain any network services that allow trusted IT products to initiate a connection to the TOE.

6.1.5.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations defined in** Table 42 **on** the **TSF Data defined in Table 42** to **U.ADMINISTRATOR**.

Table 42: Management of TSF data

TSF Data	**Operation(s)**	**Application note**
Device Administrator Password	query, set, modify, clear	In the evaluated configuration, the Device Administrator Password must be set. The query operation reads the status (set or not set) of the Device Administrator Password and not the value of the Device Administrator Password.
CA certificates	query, install, delete, export	<none>
Identity certificates	query, install, delete, export	In the evaluated configuration, an identity certificate with private key that is generated outside the TOE must be imported into the TOE's certificate store. The query operation does not allow reading of the private key associated with an identity certificate. If the private key associated with an identity certificate is marked as non-exportable, the export operation will export an identity certificate without its associated private key.
Network identity certificate	query, modify	The query operation does not allow reading of the private key associated with the network identity certificate.

6.1.5.4 Specification of management functions (FMT_SMF.1)

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

- **Management of Control Panel user authorization (FMT_MOF.1)**
- **Management of Windows Sign In (FMT_MOF.1)**
- **Management of LDAP Sign In (FMT_MOF.1)**
- **Management of account lockout policy for Local Administrator account (FMT_MOF.1)**
- **Management of Inactivity Timeout for Control Panel sign-in sessions (FMT_MOF.1)**
- **Management of enhanced security event logging (FMT_MOF.1)**
- **Management of IPsec (FMT_MOF.1)**
- **Management of IPsec/Firewall address templates (FMT_MSA.1)**

- **Management of permission sets (FMT_MSA.1)**
- **Management of permissions associated with permission sets (FMT_MSA.1)**
- **Management of IPsec/Firewall service templates (FMT_MSA.1)**
- **Management of Device Administrator Password (FMT_MTD.1)**
- **Management of CA certificates (FMT_MTD.1)**
- **Management of identity certificates (FMT_MTD.1)**
- **Management of network identity certificate (FMT_MTD.1)**

6.1.5.5 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

- **System Clock - Timestamp 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

- **Device Administrator Password**
- **Windows Sign In settings**
- **LDAP Sign In settings**
- **Permission sets**

- **Permissions associated with permission sets**
- **Network user to permission set relationships**
- **Network group to permission set relationships**
- **"Allow users to choose alternate sign-in methods at the product control panel" function enable/disable setting**

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 TSF-initiated termination of Control Panel sign-in session (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive *Control Panel sign-in* session after ~~a~~ **an administrator-configurable amount 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.

Table 43: Mapping of security functional requirements to security objectives

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT.LOGGED
FAU_GEN.2	O.AUDIT.LOGGED

Security functional requirements	Objectives
FCS_CKM.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_CKM.1-job	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.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, O.DOC.NO_DIS, O.FUNC.NO_ALT
FCS_COP.1-tst	O.SOFTWARE.VERIFIED
FCS_RBG_EXT.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FDP_ACC.1-cac	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT

Security functional requirements	Objectives
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, O.PROT.NO_ALT, O.USER.AUTHORIZED
FIA_USB.1	O.USER.AUTHORIZED

Security functional requirements	Objectives
FMT_MOF.1	O.PROT.NO_ALT
FMT_MSA.1	O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.USER.AUTHORIZED
FMT_MTD.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.PROT.NO_ALT
FMT_SMF.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT
FMT_SMR.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.USER.AUTHORIZED
FPT_FDI_EXP.1	O.INTERFACE.MANAGED
FPT_STM.1	O.AUDIT.LOGGED
FPT_TST.1	O.SOFTWARE.VERIFIED
FTA_SSL.3	O.INTERFACE.MANAGED, O.USER.AUTHORIZED
FTP_ITC.1	O.CONF.NO_ALT, O.CONF.NO_DIS, O.DOC.NO_ALT, O.DOC.NO_DIS, O.FUNC.NO_ALT, O.PROT.NO_ALT

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:

Table 44: Security objectives for the TOE rationale

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-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel that detects unauthorized modification. • FCS_COP.1-ipsec which specifies the SHA and HMAC cryptographic algorithms used by IPsec to detect unauthorized modification. • FCS_RBG_EXT.1 which specifies the random bit generation used by IPsec. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MTD.1 which enforce protection by restricting access. • FMT_SMF.1 which supports control of security attributes by requiring functions to control attributes.

Security objectives	Rationale
	• 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-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel protected from unauthorized disclosure. • FCS_COP.1-ipsec which specifies the RSA signature generation and verification along with the AES and HMAC cryptographic algorithms used by IPsec to help prevent unauthorized disclosure. • FCS_RBG_EXT.1 which specifies the random bit generation used by 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 which enforce protection by restricting access. • FMT_SMF.1 which supports control of security attributes by requiring functions to control attributes. • FMT_SMR.1 which supports control of security attributes by requiring security roles. • FTP_ITC.1 which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.DOC.NO_ALT	The objective: • The TOE shall protect User Document Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment.

Security objectives	**Rationale**
	• FCS_CKM.1-job which specifies the PBKDF2 with HMAC-SHA256 used by the TOE to process encrypted stored print jobs. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel that detects unauthorized modification. • FCS_COP.1-ipsec which specifies the SHA and HMAC cryptographic algorithms used by IPsec to detect unauthorized modification. • FCS_COP.1-job which specifies the SHA and HMAC cryptographic algorithms used by the TOE to unlock encrypted stored print jobs and the AES decryption cryptographic algorithm used by the TOE to decrypt encrypted stored print jobs. • FCS_RBG_EXT.1 which specifies the random bit generation used by 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 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-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment.

Security objectives	Rationale
	• FCS_CKM.1-job which specifies the PBKDF2 with HMAC-SHA256 used by the TOE to process encrypted stored print jobs. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel protected from unauthorized disclosure. • FCS_COP.1-ipsec which specifies the RSA signature generation and verification along with the AES and HMAC cryptographic algorithms used by IPsec to help prevent unauthorized disclosure. • FCS_COP.1-job which specifies the SHA and HMAC cryptographic algorithms used by the TOE to unlock encrypted stored print jobs and the AES decryption cryptographic algorithm used by the TOE to decrypt encrypted stored print jobs. • FCS_RBG_EXT.1 which specifies the random bit generation used by IPsec. • FDP_ACC.1-cac which enforces protection by establishing an access control policy. • FDP_ACF.1-cac which supports access control policy by providing access control function. • FDP_RIP.1 which enforces protection by making residual data unavailable. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MSA.1 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.

Security objectives	Rationale
O.FUNC.NO_ALT	The objective: • The TOE shall protect User Function Data from unauthorized alteration. is met by: • FCS_CKM.1-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment. • FCS_CKM.1-job which specifies the PBKDF2 with HMAC-SHA256 used by the TOE to process encrypted stored print jobs. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel that detects unauthorized modification. • FCS_COP.1-ipsec which specifies the SHA and HMAC cryptographic algorithms used by IPsec to detect unauthorized modification. • FCS_COP.1-job which specifies the SHA and HMAC cryptographic algorithms used by the TOE to unlock encrypted stored print jobs and the AES decryption cryptographic algorithm used by the TOE to decrypt encrypted stored print jobs. • FCS_RBG_EXT.1 which specifies the random bit generation used by 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 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.

Security objectives	Rationale
O.INTERFACE.MANAGED	The objective: • The TOE shall manage the operation of external interfaces in accordance with security policies. is met by: • FIA_UAU.1 and FIA_UAU.2 which enforce management of external interfaces by requiring user authentication. • FIA_UID.1 and FIA_UID.2 which enforce management of external interfaces by requiring user identification. • 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-ipsec which specifies the type of cryptographic keys generated for IPsec key establishment. • FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel that detects unauthorized modification. • FCS_COP.1-ipsec which specifies the SHA and HMAC cryptographic algorithms used by IPsec to detect unauthorized modification. • FCS_RBG_EXT.1 which specifies the random bit generation used by IPsec. • FIA_UID.1 and FIA_UID.2 which support access control and security roles by requiring user identification. • FMT_MOF.1 which specifies the roles that can manage the security functions. • FMT_MTD.1 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.

Security objectives	Rationale
	• FTP_ITC.1 which enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.SOFTWARE.VERIFIED	The objective: • The TOE shall provide procedures to self-verify executable code in the TSF. is met by: • FPT_TST.1 which enforces verification of software by requiring the TOE include self-tests. • FCS_COP.1-tst which specifies the SHA cryptographic algorithm used for TSF self-testing.
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 locks Device Administrator account (a.k.a. Local Administrator account) after an administrator configurable positive integer of unsuccessful Control Panel authentication attempts via Local Device Sign In method. • 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 which support access control function by enforcing control of security attributes. • FMT_SMR.1 which supports authorization by requiring security roles.

Security objectives	Rationale
	- FTA_SSL.3 which enforces authorization by terminating inactive sessions.

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:

Table 45: TOE SFR dependency analysis

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FCS_CKM.1-ipsec	[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.1-job	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1-job
	FCS_CKM.4	This dependency is unresolved. The derived 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-ipsec
	FCS_CKM.4	This dependency is unresolved. The derived keys are not formally destroyed. The object reuse mechanisms of the operating system prevent their use except in the intended context.

Security functional requirement	Dependencies	Resolution
FCS_COP.1-ipsec	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. The RSA keys used by the TOE for IPsec authentication are generated outside the TOE in the operational environment and imported into the TOE. The IPsec session keys are generated by FCS_CKM.2.
	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]	FCS_CKM.1-job
	FCS_CKM.4	This dependency is unresolved. The derived keys are not formally destroyed. The object reuse mechanisms of the operating system prevent their use except in the intended context.
FCS_COP.1-tst	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. There are no keys generated for or used by this hash algorithm.
	FCS_CKM.4	This dependency is unresolved. There are no keys used by this hash algorithm, thus, there are no keys to destroy.
FCS_RBG_EXT.1	No dependencies	
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

Security functional requirement	Dependencies	Resolution
		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	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[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_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	

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

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 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.).

Table 46: Security assurance requirements

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.3 Functional specification with complete summary	CC Part 3	No	No	No	No
	ADV_TDS.2 Architectural 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.3 Authorisation controls	CC Part 3	No	No	No	No
	ALC_CMS.3 Implementation representation CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ALC_DVS.1 Identification of security measures	CC Part 3	No	No	No	No
	ALC_FLR.2 Flaw reporting procedures	CC Part 3	No	No	No	No
	ALC_LCD.1 Developer defined life-cycle model	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
	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.2 Analysis of coverage	CC Part 3	No	No	No	No
	ATE_DPT.1 Testing: basic design	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

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 [PP2600.1]. 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 [PP2600.1].

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.

To generate the proper set of audit events, the TOE's enhanced security event logging must be enabled.

The complete audit record format and audit record details are provided in the [CCECG] in chapter *7 Enhanced security event logging messages* in section *Syslog messages*. The [CCECG] groups the events into event categories in the section *Syslog messages*.

The following table provides a mapping of the [CCECG] event categories to the events defined in FAU_GEN.1. (The ST author's intent is to not consume 30 pages of the ST by repeating the audit events listed in the [CCECG], but to refer the ST reader to the appropriate category of events in the [CCECG] that map to the events defined in FAU_GEN.1.).

Table 47: TOE audit records

Auditable event	**CCECG “*Syslog messages*” category and records**
Start-up and shutdown of the audit functions	Enhanced security event logging: • Auditing was started during boot up • Auditing was stopped via the EWS • Auditing was restarted via the EWS
Job completion	Job completion: • Copy job completion • Email job completion • Save (scan) to SharePoint job completion • Save (scan) to Network Folder job completion • Fax Send job completion • Fax Receive job completion • Save to Device Memory job completion • Retrieve from Device Memory job completion (Print from job storage) • Job Notification completion • Print job completion
Both successful and unsuccessful use of the authentication mechanism	Control panel sign in (Local Device): • Sign in using the Local Device sign-in method successful for the specified user • Sign in using the Local Device sign-in method failed
	Control panel sign in (Windows): • Sign in using the Windows sign-in method successful for the specified user • Sign in using the Windows sign-in method failed for the specified user
	Control panel sign in (LDAP): • Sign in using the LDAP sign-in method successful for the specified user • Sign in using the LDAP sign-in method failed for the specified user

Auditable event	**CCECG "*Syslog messages*" category and records**
Both successful and unsuccessful use of the identification mechanism	Same categories and records as the "Both successful and unsuccessful use of the authentication mechanism" auditable events
Use of the management functions	Device administrator password: • Device Administrator Password modified
	Windows Sign In: • Windows Sign In enabled • Windows Sign In disabled • Windows Sign In configuration modified
	LDAP Sign In: • LDAP Sign In enabled • LDAP Sign In disabled • LDAP Sign In configuration modified
	Allow users to choose alternate sign-in methods at the product control panel: • Sign In and Permission Policy settings modified
	Account lockout policy for device administrator account: • Account Lockout Policy enabled • Account Lockout Policy disabled • Account Lockout Policy setting modified
	Control panel inactivity timeout: • Control Panel Inactivity Timeout Changed
	Custom permission sets: • Permission Set added • Permission Set modified • Permission Set copied • Permission Set deleted
	Permissions associated with permission sets: • Permission Set modified

Auditable event	**CCECG "*Syslog messages*" category and records**
	CA certificates: • Device CA certificate installed • Device CA certificate deleted
	Identity certificates: • Device Identity certificate and private key installed • Device Identity certificate for network identity selected • Device Identity certificate deleted
	IPsec/Firewall address templates: • IPsec/Firewall address policy added • IPsec/Firewall address policy modified • IPsec/Firewall address policy deleted
	IPsec/Firewall service templates: • IPsec/Firewall service policy added • IPsec/Firewall service policy modified • IPsec/Firewall service policy deleted
Modifications to the group of users that are part of a role	Network user to permission set relationships: • User to Permission Set Relationship added • User to Permission Set Relationship deleted
	Network group to permission set relationships: • Group to Permission Set Relationship added • Group to Permission Set Relationship deleted
	IPsec/Firewall rules: • IPsec/Firewall rule added • IPsec/Firewall rule deleted • IPsec/Firewall rule enabled • IPsec/Firewall rule disabled • IPsec/Firewall rule position changed
Changes to the time	System time: • System time changed

Auditable event	**CCECG *"Syslog messages"* category and records**
Failure of the trusted channel functions	IKEv1 phase 1 negotiations: • IKEv1 phase 1 negotiation failed initiated by the client computer • IKEv1 phase 1 negotiation failed initiated by the local device (TOE)
	IKEv1 phase 2 negotiations: • IKEv1 phase 2 negotiation failed initiated by the client computer • IKEv1 phase 2 negotiation failed initiated by the local device (TOE)
	IKEv2 phase 1 negotiations: • IKEv2 phase 1 negotiation failed initiated by the client computer • IKEv2 phase 1 negotiation failed initiated by the local device (TOE)
	IKEv2 phase 2 negotiations: • IKEv2 phase 2 negotiation failed initiated by the client computer • IKEv2 phase 2 negotiation failed initiated by the local device (TOE)
	IPsec ESP: • IPsec using ESP failed
Termination of an interactive session by the session termination mechanism	Control panel user sign out: • Control Panel session terminated

Each audit 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.

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 "\". 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 is used to supply the cryptographic algorithms for IPsec. See section 7.1.7 for more information.

The TOE supports the decrypting of an encrypted stored print job. To decrypt an encrypted stored print job, the TOE derives a key from a Job Encryption Password and unlocks the decryption key using the derived key. The TOE then decrypts the encrypted stored print job using the decryption key. The key derivation code and the decryption code used by the TOE is included in the TOE. See section 7.1.4.3 for more information.

The TOE’s on-demand Data Integrity Test uses the SHA-256 algorithm to verify the integrity of specific TSF Data. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA2-256 algorithm. See section 7.1.5.2 for more information.

The TOE’s on-demand Code Integrity Test uses the SHA-256 algorithm to verify the integrity of TOE executable code files stored on the storage drive. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA2-256 algorithm. See section 7.1.5.2 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 (Local Administrator account only)

- 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 perform the following functions:

- Viewing of help information
- Viewing of device status information
- Viewing of network connectivity status information
- Viewing of system time
- Viewing of Web Services status information
- Viewing of Welcome screen
- Selection of Sign In
- Selection of sign-in method from Sign In screen
- Printing of help information
- Printing of network connectivity status information
- Changing language for the session
- Resetting of session

The TOE contains a local user database that defines a single administrative (U.ADMINISTRATOR) device user account called the Local Administrator account to support the Local Device Sign In mechanism. The Local Administrator account contains the following attributes:

- Display Name
- Administrator Access Code
- Permission Set

The Display Name and Permission Set attributes for the Local Administrator account are hardcoded. There values are:

- Display Name = admin
- Permission Set = Device Administrator permission set

Only the Administrator Access Code (a.k.a. Device Administrator Password) is manageable. It can be managed via the EWS. The Device Administrator Password can be set to value between 1 and 16 characters in length. Additionally, the Device Administrator Password can contain upper- and lower-case letters, numbers, and the following special characters:

- "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", """, "'", "`", "+", ",", "-", ".", "/", "\", ":", ";", "<", "=", ">", "?", "[", "]", "_", "|", "~", "{", "}" In the evaluated configuration, the Device Administrator Password must be at a minimum 8 characters in length and must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.

The Device Administrator Password can also be used to sign into the EWS from a remote computer in addition to signing in at the Control Panel.

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 signs 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 a dot 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 account lockout functionality to help protect against brute-force attacks. The account lockout functionality applies to the Device Administrator account (a.k.a. Local Administrator account) only.

The lockout mechanism uses the following control values.

- Account lockout maximum attempts
- Account lockout interval
- Account reset lockout counter interval

The account lockout maximum attempts value allows an administrator to control the number of failed authentication attempts on the account before it is locked. The administrator can choose a value between 3 and 10 inclusively. Consecutive failed authentication attempts using the same authentication credential count as a single failed authentication attempt. The counted failed attempts must happen within the value set for the account reset lockout counter interval value; otherwise, the maximum attempts counter is reset when the account reset lockout counter interval value elapses.

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 RSA 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 designated as the network 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 uses RSA signature generation and signature verification methods as part of this validity checking process.

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 7.1.7 for more details.

The TOE supports the following versions of the IKE protocol:

- IKEv1 ([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:

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

The Administrative Computer and Network Client Computers service templates are 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) and REST Web Services (HTTP) interfaces.

IP address management is discussed in section 7.1.4.5. Certificate management is discussed in section 7.1.7.

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 query, create, modify, and delete Permission Sets. In addition, only U.ADMINISTRATOR can query, create, modify, and delete the Permission Set associations to users. The TOE contains the following built-in Permission Sets:

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

Built-in Permission Sets cannot be renamed or deleted. The permissions associated with the Device Administrator Permission Set can be queried, but cannot be configured to deny access (i.e., the permissions are always set to grant access). The permissions associated with the Device Guest and Device User Permission Sets can be queried and can be configured to grant or deny access.

The Device Administrator Permission Set has all permissions set to grant access. In the evaluated configuration, the Device Guest Permission Set has permissions configured to deny access, and the Device User permission set has all administrative permissions configured to deny access.

The Device Administrator Permission Set is automatically granted to the Local Administrator account (U.ADMINISTROR) and can be granted to other administrator accounts (U.ADMINISTRATOR) defined in remote authentication server (e.g. LDAP server) used by remote sign-in method (e.g. LDAP Sign In).

The Device Guest Permission Set is associated with a Control Panel session when no user signed in. In the evaluated configuration, the Device Guest Permission Set has all permissions configured to deny access. With all permissions in the Device Guest Permission Set configured to deny access, the TOE requires all users to sign in at the Control Panel in order to perform any document-processing or administrative functions at the Control Panel.

Permissions in a Permission Set include permissions as high-level as executing the Print from Job Storage application. They also include more granular permissions that control administrative functions like the ability to delete protected jobs in Job Storage without entering a Job Encryption Password or Job PIN. Each permission in a Permission Set has two possible values: deny access and grant access.

This section maps to the following SFRs:

- FMT_MSA.1
- 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 the time of creation. 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 job is first encrypted with AES-256 in CBC mode using an encryption/decryption key and protected with a key derived from the user-specified Job Encryption Password. The stored print job is then sent encrypted to the TOE and stored encrypted by the TOE. To decrypt the encrypted stored print job at the Control Panel, a user must enter the correct Job Encryption Password that was used to derive the key to protect the job. The key derivation function and decryption algorithm are 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_CKM.1-job
- 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 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 jobs (D.DOC) 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 (read/delete D.DOC) received 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.

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 to TOE functions available at the Control Panel using permissions defined in Permission Sets. During the Control Panel sign-in process, the TOE authorizes the user after they are successfully identified and authenticated. As part of the user authorization process, the TOE associates Permission Sets to the user and then applies a Permission Set (which is the combination of the Permission Sets associated to the user). The applied Permission Set (a.k.a. session Permission Set) becomes the user's User Role. Access to each TOE function is configurable via a permission in Permission Sets by an administrator. A user can perform any function permitted in the session Permission Set. Control Panel applications (e.g., Copy, Fax, Print from Job Storage) use the user's session 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 [PP2600.1] functions of F.CPY, F.DSR, F.FAX, F.PRT, F.SCN, and F.SMI as determined by the user's session 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 a feature called “Allow users to choose alternate sign-in methods at the product’s control panel” which allows administrators to select if the sign-in method application mappings are enforced or ignored by the TOE. This feature can be enabled or disabled through the EWS (HTTP). When this feature is disabled, the TOE enforces the "sign-in method to application" mappings and prunes (reduces) the user's session Permission Set accordingly. When this feature 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 [PP2600.1] 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 does not allow forwarding of data to an External Interface. The TOE contains only one External Interface in the evaluated configuration and that interface is the Shared-medium Interface. The terms External Interface and Shared-medium Interface are defined in [PP2600.1] 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. In the evaluated configuration, the forwarding of data functionality is disabled.

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.

This section maps to the following SFR:

- FPT_FDI_EXP.1

7.1.5.2 TSF Self-Testing

TSF Functional tests

The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of correct operations tests. These correct operation tests 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:

- System Clock - Timestamp verification
- LDAP Settings verification
- Windows Setting verification

TSF Data Integrity Test

The Data Integrity Test provides the administrator (U.ADMINISTRATOR) the ability to verify the integrity of certain TSF data on-demand. The administrator first sets a reference point and then the administrator can periodically perform the test to verify the integrity of the current TSF data against the reference point. The EWS interface allows the administrator to set the reference point and execute the Data Integrity Test.

The Data Integrity Test uses the SHA-256 algorithm for both setting the reference point and verifying the integrity of current TSF Data against the reference point.

TSF Code Integrity Test

The Code Integrity Test provides the administrator (U.ADMINISTRATOR) the ability to verify the integrity of TOE executable code files stored on the storage drive on-demand. The administrator first sets a reference point and then the administrator can periodically perform the test to verify the integrity of the current TOE executable code files against the reference point. The EWS interface allows the administrator to set the reference point and execute the Code Integrity Test.

The Code Integrity Test uses the SHA-256 algorithm for both setting the reference point and verifying the integrity of current TOE executable code files against the reference point.

This section maps to the following SFR:

- FCS_COP.1-tst
- FPT_TST.1

7.1.5.3 Reliable Timestamps

The TOE contains a system clock that is used to generate reliable timestamps. In the evaluated configuration, the administrator must configure the TOE to synchronize its system clock with a Network Time Protocol (NTP) server.

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

7.1.6.1 Inactivity Timeout

The TOE supports an inactivity timeout for Control Panel sign-in sessions. If a signed in user is inactive for longer than the specified period of inactivity, the user is automatically signed out of the Control Panel by the TOE. The inactivity period is managed by the administrator through EWS (HTTP) or the Control Panel. Only one inactivity period setting exists per TOE.

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).

Table 48: Trusted channel connections

Secure protocol	Network channel	Initiated by
IPsec	Email connections (SMTP gateway)	TOE
	EWS (HTTP) connections (including web browser & certificate upload)	Administrative Computer
	REST Web Services (HTTP) connections	Administrative Computer
	Windows domain controller (Kerberos) connections	TOE
	LDAP server connections	TOE
	NTP connections	TOE
	PJL connections	Administrative Computer & Network Client Computer
	Scan to Network Folder connections (SMB, FTP)	TOE
	Scan to SharePoint connections	TOE
	Syslog server connections	TOE
	DNS server connections	TOE
	WINS server connections	TOE

The TOE uses IPsec as means to provide trusted channel communications. IPsec uses X.509v3 certificates, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (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 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 2048-bit, and 3072-bit signature generation and verification
- DSA 2048-bit, 3072-bit, 4096-bit, 6144-bit, and 8192-bit key pair generation
- DH (IKEv1, IKEv2) key establishment/exchange
- AES-128, AES-192, and AES-256 in CBC mode for data transfers
- AES-256 (with ECB mode) for the CTR_DRBG(AES)
- CTR_DRBG(AES)
- SHA-1, SHA-256, SHA-384, and SHA-512 hashing
- HMAC-SHA1-96
- HMAC-SHA-256-128
- HMAC-SHA-384-192
- HMAC-SHA-512-256

IPsec is conformant to the MUST/MUST NOT requirements of the following Internet Engineering Task Force (IETF) Request for Comments (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 the following X.509v3 certificates for IPsec in the certificate store:

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

The EWS (HTTP) interface allows administrators to manage these X.509v3 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 with private key and designate it 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 install and delete CA certificates used by IPsec.

This section maps to the following SFRs:

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

7.1.8 CAVP Certificates

Table 49 contains a complete list of cryptographic operations and their CAVP certificates claimed by this ST.

Table 49: CAVP certificates

Usage	**Implementation**	**SFR**	**Standard and operation**	**CAVP certificate**
IPsec with IKEv1 and IKEv2	HP FutureSmart QuickSec 5.1	FCS_CKM.1-ipsec	*[FIPS PUB 186-4]* KAS FFC DSA L=2048, N=224 L=2048, N=256 L=3072, N=256 Prerequisite: SHS #4474, DRBG #2220	DSA #1432
		FCS_CKM.2	*[NIST SP 800-56A]* KAS FFC DH (dhEphem) KARoles: Initiator, Responder	CVL #1999

Usage	Implementation	SFR	Standard and operation	CAVP certificate
			FB: SHA: SHA2-256 FC: SHA: SHA2-256 Prerequisite: SHS #4474, DSA #1432, DRBG #2220	
		FCS_COP.1-ipsec	*[FIPS PUB 197 (AES) and NIST SP 800-38A (CBC, ECB)]* AES-CBC Modes: Decrypt, encrypt Key lens: 128, 256 (bits) AES-ECB Modes: Encrypt Key lens: 256 (bits)	AES #5567
			[FIPS PUB 186-4] RSA 186-4 *Signature generation PKCS1.5* Mod 2048 SHA: SHA2-256, SHA2-384, SHA2-512 Mod 3072 SHA SHA2-256, SHA2-384,	RSA #2996

Usage	Implementation	SFR	Standard and operation	CAVP certificate
			SHA2-512 *Signature verification PKCS1.5* Mod 2048 SHA SHA-1, SHA2-256, SHA2-384, SHA2-512 Mod 3072 SHA SHA-1, SHA2-256, SHA2-384, SHA2-512 Prerequisite: SHS #4474, DRBG #2220	
			[FIPS 180-3 and 180-4] SHA-1, SHA2-256, SHA2-384, SHA2-512	SHS #4474
			[FIPS 198-1] HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	HMAC #3711

Usage	Implementation	SFR	Standard and operation	CAVP certificate
			Prerequisite: AES #5567	
		FCS_RBG_EXT.1	*[NIST SP 800-90A Rev 1]* CTR_DRBG(AES) Counter Modes: AES-256 (Uses AES-ECB-256) Prerequisite: AES #5567	DRBG #2220
TSF self-testing	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	FCS_COP.1-tst	*[FIPS 180-3 and 180-4]* SHA-256	SHS #4474

7.1.9 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 Print from Job Storage 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 at the product’s control panel" feature.

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 protected using a key derived from the Job Encryption Password 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
- FMT_MSA.1
- FMT_MTD.1
- 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
BIOS	Basic Input/Output System
CA	Certificate Authority
CBC	Cipher Block Chaining
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
MD5	Message Digest 5
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
REST	Representational State Transfer
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 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

FIPS197 **Advanced Encryption Standard**

Date 2001-11-26

Location http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS186-4 **Digital Signature Standard (DSS)**

Date 2013-07-19

Location https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS180-4 **Secure Hash Standard (SHS)**

Date 2015-08-04

Location https://csrc.nist.gov/publications/detail/fips/180/4/final

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

Author(s) RSA Laboratories

Version 1.5

Date November 1993

PKCS5v2.1 **PKCS5v2.1: Password-Based Cryptography Standard**

Author(s) RSA Laboratories

Version 2.1

Date October 2012

PP2600.1 **IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A"**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-CPY **SFR Package for Hardcopy Device Copy (CPY) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-DSR **SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-FAX **SFR Package for Hardcopy Device Document Fax (FAX) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-PRT **SFR Package for Hardcopy Device Print (PRT) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-SCN **SFR Package for Hardcopy Device Scan (SCN) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

PP2600.1-SMI **SFR Package for Hardcopy Device Shared-medium Interface (SMI) Functions**

Version 1.0

Date June 2009

Location https://www.niap-ccevs.org/pp/pp_hcd_br_v1.0.pdf

QuickSec51 **QuickSec 5.1 Toolkit Reference Manual**

Author(s) INSIDE Secure

Version 1..0

Date December 2009

RFC1321 **The MD5 Message-Digest Algorithm**

Author(s) R. Rivest

Date 1992-04-01

Location http://www.ietf.org/rfc/rfc1321.txt

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

CCECG **Common Criteria Evaluated Configuration Guide for HP Multifunction Printers**

HP Color LaserJet Enterprise MFP M776,
HP LaserJet Enterprise MFP M634/M635/M636

Author(s) HP Inc.

Edition 1

Date 4/2021

M776-UG **HP Color LaserJet Enterprise MFP M776**

User Guide

Author(s) HP Inc.

Edition 1

Date 10/2019

M776DN_Z-IG **HP Color LaserJet Enterprise MFP M776dn, M776z**

M776dn
M776z

Installation Guide

Author(s) HP Inc.

Date 2019

M776ZS-IG **HP Color LaserJet Enterprise MFP M776zs**

M776zs

Installation Guide

Author(s) HP Inc.

Date 2019

M634_5_6-UG **HP LaserJet Enterprise MFP M634**
HP LaserJet Enterprise MFP M635
HP LaserJet Enterprise MFP M636

User Guide

Author(s) HP Inc.

Edition 1

	Date	5/2020
M634_5_6-IG	**HP LaserJet Enterprise MFP M634** **HP LaserJet Enterprise MFP M635** **HP LaserJet Enterprise MFP M636** **M634dn, M634h, M634z, M635h, M635fht, M635z, M636fh, M636z** **Installation Guide**	
	Author(s)	HP Inc.
	Date	2020