HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner

Security Target

Version:	2.0
Status:	Final
Last update:	2019-03-28

Trademarks

The following terms are trademarks of Arm Holdings plc in the United States, other countries, or both.

- Arm®
- Cortex®

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

- atsec®

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

- HP®
- LaserJet®

The following terms are trademarks of INSIDE Secure in the United States, other countries, or both.

- INSIDE Secure®
- QuickSec®

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®
- Windows Mobile®

The following terms are trademarks of the OpenSSL Software Foundation in the United States, other countries, or both.

- OpenSSL®

The following terms are trademarks of the Seagate Technology LLC in the United States, other countries, or both.

- Seagate®
- Seagate Secure®

The following term is a trademark of the Trusted Computing Group in the United States, other countries, or both.

- Trusted Computing Group®

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

Legal Notices

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
2.0	2019-03-28	Gerardo Colunga, Anthony Peterson	Final version.

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

Title:	HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target
Version:	2.0
Status:	Final
Date:	2019-03-28
Sponsor:	HP Inc.
Developer:	HP Inc.
Certification Body:	CSEC
Certification ID:	CSEC 2018007
Keywords:	Common Criteria, HCD, HCDPP, Hardcopy Device, LaserJet, Scanner, Digital Sender, ScanJet

1.2 TOE Identification

The TOE is the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner. The TOE models and firmware versions are provided in Table 1.

1.3 TOE Type

The TOE type is a hardcopy device (HCD) which provides the functionality of a document capture workstation, also known as a scanner.

1.4 TOE Overview

This document is the Common Criteria (CC) Security Target (ST) for the HP Inc. products listed in Section 1.2 evaluated as HCDs in compliance with the Protection Profile for Hardcopy Devices Version 1.0, dated September 10, 2015 [HCDPP].

The TOE is an HCD including internal firmware, but exclusive of non-security relevant options such as finishers. The TOE also includes the English-language guidance documentation.

The following firmware modules are included in the TOE.

- System firmware
- Jetdirect Inside firmware

The System firmware controls all functionality except for the network-related functionality. The Jetdirect Inside firmware controls all network-related functionality from Ethernet to Internet Protocol Security (IPsec). These firmware modules are bundled into a single installation bundle.

Two models of HCDs are included in this evaluation. Physically speaking, both models use the same mainboard and processor. Both models contain one field-replaceable, nonvolatile drive. Both models also have a Control Panel for operating the HCD locally and Ethernet network capability for connecting to a network. They all support remote administration over the network. The main physical differences between models are size of paper feeders and the location of the power button.

A complete list of TOE models and firmware versions is provided in Section 1.5.1.

As per [HCDPP] Section 1.5, the major security functions in this evaluation are as follows.

- Identification, authentication, and authorization to use HCD functions
- Access control
- Data encryption (a.k.a. cryptography)
- Trusted communications
- Administrative roles
- Auditing
- Trusted operation

1.4.1 Required and optional non-TOE hardware and software

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

- A Domain Name System (DNS) server
- A Network Time Service (NTS) server
- One administrative client computer network connected to the TOE in the role of an Administrative Computer. It must contain:
    - A web browser
- One or both of the following:
    - A Lightweight Directory Access Protocol (LDAP) server
    - A Windows domain controller/Kerberos server
- A syslog server
- A Windows Internet Name Service (WINS) server

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

- Microsoft SharePoint ('Flow' models only)
- The following remote file systems:
    - File Transfer Protocol (FTP)
    - Server Message Block (SMB)
- A Simple Mail Transfer Protocol (SMTP) gateway

1.4.2 Intended method of use

This evaluation covers an information processing environment in which a basic 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 scanning. The physical environment should be reasonably controlled and/or monitored where physical tampering of the HCDs would be evident and noticed.

The TOE is connected to a local area network using HP's Jetdirect Inside in the evaluated configuration. The evaluated configuration uses secure network mechanisms for communication between the TOE and network computers. The TOE is managed by one designated administrative computer. Only the administrative computer can connect to the TOE. The TOE can initiate connections to trusted IT entities (e.g. SMTP gateway) to request or send information to them. The TOE is not intended be connected to the Internet.

The following list contains the use cases found in [HCDPP] Section 1.4 "Security Use Cases of the HCD" supported by the TOE.

- Required use cases
    - Scanning
    - Configuration
    - Auditing
    - Verifying software updates
    - Verifying HCD function
- Conditionally mandatory use cases
    - Field-replaceable nonvolatile storage devices
- Optional use cases
    - Image overwrite

1.5 TOE Description

This section contains a more detailed description of the TOE.

1.5.1 TOE models and firmware versions

Table 1 shows the HCD models included in this evaluation. The table also shows the 'flow' model designation, which can be found in the product name. Flow models have the ability to connect to Microsoft SharePoint servers whereas non-flow models do not.

Also as indicated in Table 1, depending on the option code purchased, the model may require the installation of one HP High-Performance Secure Hard Disk assembly (HP part #: B5L29-67903) prior to deployment. This assembly replaces one field-replaceable, nonvolatile storage drive with a field-replaceable, nonvolatile, Federal Information Processing Standard (FIPS) 140-2 validated, disk-based, self-encrypting drive (SED). The table provides the quantity of B5L29-67903 assemblies required per model.

Each model has a unique product number. The product number is the number used when ordering an HCD. Each product number can have multiple option codes associated with it when ordering. Option codes are used to specify items like 110V versus 220V power connections or whether or not the HCD comes with an SED.

For some models, certain product number and option code combinations are shipped with the same drive used in the B5L29-67903 assembly pre-installed as the field-replaceable, nonvolatile storage drive. Therefore, these models do not need a B5L29-67903 assembly. For example in Table 1, product number L2762A with option code #201 comes with the B5L29-67903 drive pre-installed, thus, the B5L29-67903 assembly is not required for this product number and option code combination. But product number L2762A with any other option code requires the installation of one of the B5L29-67903 assemblies.

All TOE models use the same Jetdirect Inside firmware version.

1) JSI24060306

The TOE includes the following System firmware versions.

2) 2406249_032755

3) 2406249_032756

Table 1 includes a mapping of the System firmware versions to the TOE models.

Product family	Model	Product number	Option codes	Qty of part # B5L29-67903 required	System firmware version
HP Digital Sender Flow 8500 fn2 Document Capture Workstation	8500 fn2	L2762A	#201	0	2406249_032755
			All other codes	1	
HP ScanJet Enterprise Flow N9120 fn2 Document Scanner	N9120 fn2	L2763A	#201	0	2406249_032756
			All other codes	1	

Table 1: TOE hardware and firmware reference

Table 2 contains the TOE's English-guidance documentation reference.

Models	Title	Reference
All models	Preparatory Procedures and Operational Guidance for the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner	[CCECG]
All models	HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide	[8500_N9120-UG]
All models	HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide	[8500_N9120-IG]

Table 2: TOE English-guidance documentation reference

Table 3 shows the operating system and processor used by all TOE models.

OS	Windows Embedded CE 6.0 R3
Processor	Arm Cortex-A8

Table 3: TOE OS and processor

1.5.2 Architecture

The TOE is designed to be shared by many human users. It performs the functions of scanning and sending of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration except when the administrator performs trusted update via the USB).

[HCDPP] defines the TOE's physical boundary as the entire HCD product with the possible exclusion of physical options and add-ons that are not security relevant.

Operating system and processor

The TOE's operating system is the Windows Embedded CE 6.0 R3 running on an Arm Cortex-A8 processor.

Networking

The TOE supports Local Area Network (LAN) capabilities. The LAN is used to communicate with the administrative computer and trusted IT entities.

The TOE protects all network communications with IPsec, which is part of the Jetdirect Inside firmware. It implements Internet Key Exchange version 1 (IKEv1) and supports both pre-shared key (PSK) authentication and X.509v3 certificate-based authentication. The TOE supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

Administrative Computer and administrative interfaces

The Administrative Computer connects to the TOE using IPsec. This computer can administer the TOE using the following interfaces over the IPsec connection.

- Embedded Web Server (EWS)
- Representational state transfer (REST, a.k.a. RESTful) Web Services

EWS

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

RESTful

The Web Services (WS) interfaces allow administrators to externally manage the TOE. The evaluated configuration only supports the RESTful Web Services interface. The RESTful interface is protected using IPsec.

Administrative Computer

For design reasons, only one computer can be used as the Administrative Computer for the TOE in the evaluated configuration. This computer is used for administration of the TOE.

The [CCECG] section *IPsec/Firewall* describes how to properly configure the TOE to allow a single Administrative Computer.

SharePoint, FTP, and SMB

The TOE supports Microsoft SharePoint (Flow models only) and remote file systems for the storing of scanned documents. The TOE uses IPsec to protect the communication to SharePoint and to the remote file systems. For remote file system connectivity, the TOE supports the FTP and SMB protocols. (SharePoint is HTTP-based, but IPsec is used to protect the HTTP-based communications.)

SMTP mail server

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 HCD supplies to HP.

The TOE supports protected communications between itself and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec to protect the communication with the SMTP gateway. The TOE can only protect unencrypted email up to the SMTP gateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

Audit Server (syslog server)

The TOE supports the auditing of security-relevant functions by generating and forwarding audit records to an external syslog server. It supports both internal and external storage of audit records. The TOE uses IPsec to protect the communications between itself and the syslog server.

DNS, NTS, and WINS servers

The TOE requires a DNS server, an NTS server, and a WINS server in the Operational Environment. The TOE connects to them over an IPsec connection.

Control Panel

Each HCD contains a user interface (UI) called the Control Panel. The Control Panel consists of a touchscreen LCD, a physical home screen button that are attached to the HCD, and 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. Both administrative and non-administrative users can access the Control Panel.

Internal and External Authentication

Note: The terms Internal Authentication and External Authentication start with a capitalized first character to match the [HCDPP] usage of these terms.

The TOE supports the following Internal Authentication mechanisms in the evaluated configuration.

- Local Device Sign In

The TOE supports the following External Authentication mechanisms in the evaluated configuration.

- LDAP Sign In
- Windows Sign In (i.e., Kerberos)

The TOE's guidance documents and firmware refer to the following mechanisms as *sign-in methods*: Local Device Sign In, LDAP Sign In, and 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 LDAP Sign In method supports the use of an external LDAP server for authentication. The Windows Sign In method supports the use of an external Windows Domain server for authentication.

Section 1.5.3.3 provides a mapping of authentication mechanisms to TOE interfaces.

Nonvolatile Storage

All TOE models contain one field-replaceable, nonvolatile storage disk drive. This drive is a FIPS 140-2 validated SED. Depending on the TOE model, this drive may come pre-installed or the TOE may require the installation of the HP High-Performance Secure Hard Disk assembly prior to deploying the TOE.

Firmware Components

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both firmware components work together to provide the security functionality defined in this document for the TOE. They are shown as two separate components but they both share the same operating system. The operating system is part of the System firmware.

The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the System firmware. The Jetdirect Inside firmware includes IPsec and the management functions for managing this network-related feature. It 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.

1.5.3 TOE security functionality (TSF) summary

1.5.3.1 Auditing

The TOE supports both internal and external storage of audit records. The evaluated configuration requires the use of an external syslog server for external audit record storage. The connection between the TOE and the syslog server is protected using IPsec. No unauthorized access to the audit records is allowed by the TOE.

1.5.3.2 Data encryption (a.k.a. cryptography)

IPsec

The TOE's IPsec supports both pre-shared keys (PSKs) and X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange version 1 (IKEv1) protocol, and the following cryptographic algorithms: Diffie-Hellman (DH), Elliptic Curve DH (ECDH) Digital Signature Algorithm (DSA), Elliptic Curve DSA (ECDSA), Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard-Cipher Block Chaining (AES-CBC), Advanced Encryption Standard-Electronic Code Book (AES-ECB), Secure Hash Algorithm-based (SHA-based) Hashed Message Authentication Codes (HMACs), Public-Key Cryptography Standards (PKCS) #1 v1.5 signature generation and verification, and counter mode deterministic random bit generator using AES (CTR_DRBG(AES)).

It supports multiple DH groups, transport mode, and uses Main Mode for Phase 1 exchanges in IKEv1. The IKEv1 uses the DH ephemeral (dhEphem) scheme to implement the key agreement scheme finite field cryptography (KAS FFC) algorithm when establishing a protected communication channel. DSA key generation is a prerequisite for KAS FFC when using DH ephemeral. It also uses the ECDH ephemeral unified scheme to implement the key agreement scheme elliptic curve cryptography (KAS ECC) algorithm when establishing a protected communication channel. ECDSA key generation is a prerequisite for KAS ECC when using the ECDH ephemeral unified scheme. The IKEv1 uses imported RSA-based X.509v3 certificates to authenticate the connections. The RSA authentication is accomplished using the IKEv1 digital signature authentication method.

Drive-lock password

For secure storage, all TOE models contain a single field-replaceable, nonvolatile storage device. This storage device is a FIPS 140-2 validated, disk-based, self-encrypting drive (SED).

The SED in a TOE uses a 256-bit "drive-lock password" as the border encryption value (BEV) which is used to unlock the data on the drive. The BEV is generated by the TOE using a CTR_DRBG(AES-256) algorithm and is stored as a key chain of one in non-field replaceable nonvolatile storage (EEPROM) located inside the TOE. The CTR_DRBG(AES-256) uses the Advanced Encryption Standard-Counter (AES-CTR) algorithm.

Digital signatures for trusted update

The TOE uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to verify the authenticity of the signed update images. The TOE's EWS interface allows an administrator to verify and install the signed update images.

Digital signatures for TSF testing

The TOE uses digital signatures as part of its TSF testing functionality. This is described in Section 1.5.3.7.

Cryptographic implementations/modules

The TOE uses multiple cryptographic implementations to accomplish its cryptographic functions. Table 4 provides the complete list of cryptographic implementations used to satisfy the [HCDPP] cryptographic requirements and maps the cryptographic implementations to the firmware modules.

The System firmware module contains two cryptographic implementations. All System firmware module versions use the same two cryptographic implementations; therefore, the same Cryptographic Algorithm Validation

Program (CAVP) certificates for these two cryptographic implementations are valid for all System firmware module versions claimed in this ST.

The Jetdirect Inside firmware module also contains two cryptographic implementations. Only one version of the Jetdirect Inside firmware is used by the TOE; therefore, only one set of CAVP certificates for each cryptographic implementation in this module is claimed by this ST.

Table 46 contains the complete list of cryptographic operations and CAVP certificates.

Firmware module	Cryptographic implementation	Usage
Jetdirect Inside firmware	HP FutureSmart OpenSSL FIPS Object Module 2.0.4	Drive-lock password (BEV) generation
	HP FutureSmart QuickSec 5.1	IPsec
System firmware	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	TSF testing
	HP FutureSmart Rebex Total Pack 2017 R1	Trusted update

Table 4: TOE cryptographic implementations

The field-replaceable SED also contains a cryptographic implementation within the drive called the "Seagate Secure® TCG Opal SSC Self-Encrypting Drive." This implementation is based on the Trusted Computing Group's (TCG) Opal Security Subsystem Class (SSC) specification. This implementation has been separately FIPS 140-2 validated by the SED's manufacturer. The cryptographic algorithms in this implementation are not claimed in this ST.

To prevent confusion with the new SHA3 standard, this ST replaces all occurrences of SHA-256, SHA-384, and SHA-512 with SHA2-256, SHA2-384, and SHA2-512, respectively.

1.5.3.3 Identification, authentication, and authorization to use HCD functions

Table 5 shows the Internal and External Authentication mechanisms supported by the TOE in the evaluated configuration and maps the mechanisms to the interfaces that use them.

The following is a list of terms used in this ST.

Control Panel user

A user of the Control Panel UI.

EWS user

A user of the EWS interface, usually via a web browser.

RESTful user

A user of the RESTful network interface.

Authentication type	Mechanism name	Supported interfaces
Internal Authentication	Local Device Sign In	Control Panel, EWS, RESTful
External Authentication	LDAP Sign In	Control Panel, EWS
	Windows Sign In	Control Panel, EWS, RESTful

Table 5: TOE authentication mechanisms and their supported interfaces

Internal Authentication

Local Device Sign In

The Local Device Sign In method uses an internal user account database to authenticate users. The user accounts contain the following user attributes used for identification and authentication (I&A).

- Display name
- Password

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

External Authentication

LDAP Sign In

The LDAP Sign In method supports the use of an LDAP server as an External Authentication mechanism. This method uses the LDAP bind request to authenticate users. The bind request requires the user to provide a username and password that matches a valid user account defined in the LDAP server for the bind request to be successful.

Windows Sign In

The Windows Sign In method supports the user of a Windows Domain server as an External Authentication mechanism. The user must provide a valid Windows Domain username and password to be successfully logged in to the TOE. This method is based on the Kerberos network protocol.

Control Panel I&A

The HCD has a Control Panel that allows a user to physically walk up to the HCD and select a function (e.g., scan) to be performed. The Control Panel supports the following Internal Authentication mechanism.

- Local Device Sign In

Only the Device Administrator account, which is a U.ADMIN account, is available for log in through the Local Device Sign In method in the evaluated configuration. The user must select this account name and then enter the

Device Administrator's password in order to gain access. The Device Administrator's account name is generically known as a Display name.

The Control Panel supports the following External Authentication mechanisms.

- LDAP Sign In
- Windows Sign In

Non-administrative users (U.NORMAL) as well as administrators can log in to the HCD through the Control Panel using these External Authentication mechanisms.

The Control Panel allows a handful of actions (e.g., change the language, obtain help, select an authentication mechanism) to be performed prior to identifying and authenticating a user.

The Control Panel uses permission sets (PSs) to determine user roles. The Internal Authentication mechanism has one PS per user. The External Authentication mechanisms have one PS per authentication method, zero or one PS per user, and zero or one PS per network group to which the user belongs. For additional details on the permission sets, see the TOE Summary Specification (TSS) for FMT_SMR.1.

When users sign in through the Control Panel, a user's session permission bits are calculated based on several factors and then bound to the user's session. For additional details on the permission bit calculations, see the TSS for FIA_USB.1.

The Control Panel also supports an administratively configurable inactive session termination timeout.

Network Interface I&A

The EWS and RESTful interfaces are network protocols protected by IPsec and support one or more authentication mechanisms. These interfaces perform their I&A after the IPsec connection has been established.

EWS I&A

The EWS interface is an administrative-only interface that supports the following authentication mechanisms.

- Internal Authentication mechanism
    - Local Device Sign In
- External Authentication mechanisms
    - LDAP Sign In
    - Windows Sign In

The EWS interface allows the administrator to select the authentication mechanism (a.k.a. sign-in method) prior to identifying and authenticating the user.

The EWS interface uses PSs to determine user roles. A user logging in to the EWS interface must have administrative privileges in order to successfully log in. The Internal Authentication mechanism has one PS per user. The External Authentication mechanisms have one PS per authentication method, zero or one PS per user, and zero or one PS per network group to which the user belongs. For additional details on the permission sets, see the TSS for FMT_SMR.1.

When users sign in through the EWS interface, a user's session permission bits are calculated based on several factors and then bound to the user's session. For additional details on the permission bit calculations, see the TSS for FIA_USB.1.

The EWS interface also supports an administratively configurable inactive session termination timeout.

RESTful I&A

The RESTful interface is an administrative-only interface that supports the following authentication mechanism.

- Internal Authentication mechanism
    - Local Device Sign In
- External Authentication mechanism
    - Windows Sign In

The TOE does not allow any TSF-mediated actions prior to the RESTful I&A.

Authentication failure handling and authentication feedback

The following interfaces support authentication failure handling when using Internal Authentication mechanisms.

- Control Panel
- EWS
- RESTful

The following user interfaces support protected authentication feedback (i.e., the masking of passwords when being entered during authentication).

- Control Panel
- EWS

1.5.3.4 Access control

The TOE enforces access control on TSF data and User Data. Each piece of User Data is assigned ownership and access to the data is limited by the access control mechanism. The PSs used to define roles also affect the access control of each user. The access control mechanism for User Data is explained in more detail in the TSS for FDP_ACF.1.

The TOE contains one field-replaceable, nonvolatile storage device. This device is a disk-based SED whose cryptographic functions have been FIPS 140-2 validated. Together with the drive-lock password, this SED ensures that the TSF Data and User Data on the drive is not stored as plaintext on the storage device.

The TOE also supports the optional Image Overwrite function (O.IMAGE_OVERWRITE) defined in [HCDPP]. [HCDPP] limits the scope of this function to the field-replaceable, nonvolatile storage device.

The TOE refers to the image overwrite feature as "Managing Temporary Job Files." Although the TOE displays three options for image overwrite, in the evaluated configuration the administrator must select one of the following two options, both of which completely overwrite the user document data (i.e., file).

- Secure Fast Erase (overwrite 1 time)
- Secure Sanitize Erase (overwrite 3 times)

1.5.3.5 Trusted communications

The TOE uses IPsec to protect the communications between the TOE and trusted IT entities as well as between the TOE and the administrative computer. IPsec provides assured identification of the endpoints. It implements IKEv1 and transport mode. The TOE also supports both X.509v3 certificates and pre-shared keys (PSKs) for endpoint authentication. For additional details on the TOE's IPsec features, see the TSS for FCS_IPSEC_EXT.1.

1.5.3.6 Administrative roles

The TOE supports administrative and non-administrative roles. Assignment to these roles is controlled by the TOE's administrator. In the case of the Control Panel, EWS, and RESTful (Windows Sign In) interfaces, the roles are implemented as permission sets. In the case of RESTful (Local Sign In), only an administrative account exists.

In addition, the TOE provides security management capabilities for TOE functions, TSF data, and security attributes as defined by this ST.

1.5.3.7 Trusted operation

TOE updates can be downloaded from the HP Inc. website. These updates are digitally signed by HP Inc. using the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 signature generation. The TOE's EWS interface allows an administrator to install the update images. When installing an update image, the TOE validates the digital signature of the update image before installing the update image. For additional details, see the TSS for FPT_TUD_EXT.1.

The TOE contains TSF testing functionality referred to as Whitelisting to help ensure only authentic, known-good System firmware files that have not been tampered with are loaded into memory. Whitelisting uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to validate the firmware files. For additional details, see the TSS for FPT_TST_EXT.1.

1.5.4 TOE boundaries

1.5.4.1 Physical boundary

The physical boundary of the TOE is the physical boundary of the HCD product.

Optional wireless add-ons are excluded from the TOE and are not part of the evaluation.

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. This firmware bundle contains two firmware modules.

- System firmware

- Jetdirect Inside firmware

The evaluated firmware module versions are provided in Table 1.

As seen in Table 1, there are multiple System firmware versions. Notice the first set of digits in the System firmware versions are all the same, but the second set varies. The first set of digits represents the version of the OS and other code that implement the security functions of the TOE. The second set of digits represents the drivers used to control the physical features—flatbed scanner and automatic document feeder—of the TOE. Because different sets of models do not contain the exact same set of physical features, the second set of digits differs.

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.

1.5.4.2 Logical boundary

The security functionality provided by the TOE has been listed at the end of Section 1.5.3.

1.5.4.3 Evaluated configuration

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

- HP Digital Sending Software (DSS) must be disabled.
- Only one Administrative Computer is used to manage the TOE.
- HP and third-party applications cannot be installed on the TOE.
- Type A and B USB ports must be disabled.
- Remote Firmware Upgrade through any means other than the EWS and USB must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Full Authentication must be enabled (this disables the Guest role).
- SNMPv1/v2 and SNMPv3 must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- Near Field Communication (NFC) must be disabled.
- Wireless networking (WLAN) must be disabled.
- Remote Control-Panel use is disallowed.

- Local Device Sign In accounts must not be created (i.e., only the Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS):
    - Open Extensibility Platform device (OXPd) Web Services
    - WS* Web Services

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant.

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

- [HCDPP]: Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community. Version 1.0 as of 2015-09-10; exact conformance.
- [HCDPP-ERRATA]: Protection Profile for Hardcopy Devices - v1.0, Errata #1, June 2017. Version 1.0 as of 2017-06; exact 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 Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community ([HCDPP])

Table 6 contains the NIAP Technical Decisions (TDs) for this protection profile at the time of the evaluation and a statement of applicability to the evaluation.

NIAP TD	TD description	Applicability	TD reference
TD0074	FCS_CKM.1(a) Requirement in HCD PP v1.0	Not applicable. FCS_CKM.1(a) is claimed.	[CCEVS-TD0074]
TD0157	FCS_IPSEC_EXT.1.1 - Testing SPDs	Applicable. The TOE includes IPsec.	[CCEVS-TD0157]
TD0176	FDP_DSK_EXT.1.2 - SED Testing	Applicable. The TOE includes a field-replaceable SED.	[CCEVS-TD0176]
TD0219	NIAP Endorsement of Errata for HCD PP v1.0	Applicable.	[CCEVS-TD0219]
TD0253	Assurance Activities for Key Transport	Not applicable. FCS_COP.1(i) is not claimed.	[CCEVS-TD0253]
TD0261	Destruction of CSPs in flash	Applicable. The TOE stores one or more keys in flash memory.	[CCEVS-TD0261]
TD0299	Update to FCS_CKM.4 Assurance Activities	Not applicable. The "a new value of a key of the same size" is not selected in FCS_CKM.4.	[CCEVS-TD0299]

NIAP TD	TD description	Applicability	TD reference
TD0393	Require FTP_TRP.1(b) only for printing	Applicable. Because the TOE is a scan-only device that does not have a remote, non-administrative interface, FTP_TRP.1(b) is not claimed.	[CCEVS-TD0393]

Table 6: NIAP TDs

The following NIAP-CCEVS interim guidance has been included in this evaluation.

- [CCEVS-SED]: Interim Guidance for Evaluation of Self-Encrypting Drives for the Hard Copy Device Protection Profile

3 Security Problem Definition

3.1 Threat Environment

The Security Problem Definition (SPD) is delivered into two parts. This first part describes Assets, Threats, and Organizational Security Policies, in narrative form. [Brackets] indicate a reference to the second part, formal definitions of Users, Assets, Threats, Organizational Security Policies, and Assumptions, which appear in Appendix A.

Users

A conforming TOE must define at least the following two User roles:

1. Normal Users [U.NORMAL] who are identified and authenticated and do not have an administrative role.
2. Administrators [U.ADMIN] who are identified and authenticated and have an administrative role.

A conforming TOE may allow additional roles, sub-roles, or groups. In particular, a conforming TOE may allow several administrative roles that have authority to administer different aspects of the TOE.

Assets

For a User's perspective, the primary Asset to be protected in a TOE is User Document Data [D.USER.DOC]. A User's job instructions, User Job Data [D.USER.JOB] (information related to a User's Document or Document Processing Job), may also be protected if their compromise impacts the protection of User Document Data. Together, User Document Data and User Job Data are considered to be User Data.

From an Administrator's perspective, the primary Asset to be protected in a TOE is data that is used to configure and monitor the secure operation of the TOE. This kind of data is considered to be TOE Security Functionality (TSF) Data.

There are two broad categories for this kind of data:

1. Protected TSF Data, which may be read by any User but must be protected from unauthorized modification and deletion [D.TSF.PROT]; and,
2. Confidential TSF Data, which may neither be read nor modified or deleted except by authorized Users [D.TSF.CONF].

3.1.1 Threats countered by the TOE

T.UNAUTHORIZED_ACCESS

An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.

T.TSF_COMPROMISE

An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.

T.TSF_FAILURE

A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.

T.UNAUTHORIZED_UPDATE

An attacker may cause the installation of unauthorized software on the TOE.

T.NET_COMPROMISE

An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.

3.2.1.2 Personnel

A.TRUSTED_ADMIN

TOE Administrators are trusted to administer the TOE according to site security policies.

A.TRAINED_USERS

Authorized Users are trained to use the TOE according to site security policies.

3.2.1.3 Connectivity

A.NETWORK

The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.

3.3 Organizational Security Policies

P.AUTHORIZATION

Users must be authorized before performing Document Processing and administrative functions.

P.AUDIT

Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.

P.COMMS_PROTECTION

The TOE must be able to identify itself to other devices on the LAN.

P.STORAGE_ENCRYPTION

If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.

P.KEY_MATERIAL

Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

P.IMAGE_OVERWRITE

Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.

4 Security Objectives

4.1 Objectives for the TOE

O.USER_I&A

The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.

O.ACCESS_CONTROL

The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.

O.USER_AUTHORIZATION

The TOE shall perform authorization of Users in accordance with security policies.

O.ADMIN_ROLES

The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.

O.UPDATE_VERIFICATION

The TOE shall provide mechanisms to verify the authenticity of software updates.

O.TSF_SELF_TEST

The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.

O.COMMS_PROTECTION

The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.

O.AUDIT

The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.

O.STORAGE_ENCRYPTION

If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.

O.KEY_MATERIAL

The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.

O.IMAGE_OVERWRITE

Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.

4.2 Objectives for the Operational Environment

OE.PHYSICAL_PROTECTION

The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.

OE.NETWORK_PROTECTION

The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.

OE.ADMIN_TRUST

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

OE.USER_TRAINING

The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.

OE.ADMIN_TRAINING

The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

4.3 Security Objectives Rationale

4.3.1 Coverage

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

Objective	Threats / OSPs
O.USER_I&A	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUTHORIZATION
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUDIT
O.USER_AUTHORIZATION	P.AUTHORIZATION P.AUDIT
O.ADMIN_ROLES	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUTHORIZATION

Objective	Threats / OSPs
O.UPDATE_VERIFICATION	T.UNAUTHORIZED_UPDATE
O.TSF_SELF_TEST	T.TSF_FAILURE
O.COMMS_PROTECTION	T.NET_COMPROMISE P.COMMS_PROTECTION
O.AUDIT	P.AUDIT
O.STORAGE_ENCRYPTION	P.STORAGE_ENCRYPTION
O.KEY_MATERIAL	P.KEY_MATERIAL
O.IMAGE_OVERWRITE	P.IMAGE_OVERWRITE

Table 7: Mapping of security objectives to threats and policies

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

Objective	Assumptions / Threats / OSPs
OE.PHYSICAL_PROTECTION	A.PHYSICAL
OE.NETWORK_PROTECTION	A.NETWORK
OE.ADMIN_TRUST	A.TRUSTED_ADMIN
OE.USER_TRAINING	A.TRAINED_USERS
OE.ADMIN_TRAINING	A.TRAINED_USERS

Table 8: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

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

Threat	Rationale for security objectives
T.UNAUTHORIZED_ACCESS	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_COMPROMISE	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.
T.UNAUTHORIZED_UPDATE	O.UPDATE_VERIFICATION verifies the authenticity of software updates.
T.NET_COMPROMISE	O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.

Table 9: Sufficiency of objectives countering threats

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

Assumption	Rationale for security objectives
A.PHYSICAL	OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.
A.TRUSTED_ADMIN	OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.TRAINED_USERS	OE.ADMIN_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Administrators. OE.USER_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Users.
A.NETWORK	OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.

Table 10: Sufficiency of objectives holding assumptions

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

OSP	Rationale for security objectives
P.AUTHORIZATION	O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION	O.STORAGE_ENCRYPTION protects User Document Data and Confidential TSF Data stored in Field-Replaceable Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.
P.KEY_MATERIAL	O.KEY_MATERIAL protects keys and key materials from unauthorized access and ensures that they any key materials are not stored in cleartext on the device that uses those materials for its own encryption.
P.IMAGE_OVERWRITE	O.IMAGE_OVERWRITE overwrites residual image data from Field-Replaceable Nonvolatile Storage Devices after Document Processing jobs are completed or cancelled.

Table 11: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

All of the extended components definitions in this section are from [HCDPP]. Only the [HCDPP] extended components definitions used by this ST are listed in this section.

5.1 Class FAU: Security audit

5.1.1 Extended: External Audit Trail Storage (FAU_STG)

Family behaviour

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component levelling

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Management: FAU_STG_EXT.1

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

a) The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1

There are no audit events foreseen.

5.1.1.1 FAU_STG_EXT.1 - Extended: Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Rationale

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2 Class FCS: Cryptographic support

5.2.1 Extended: Cryptographic Key Management (FCS_CKM)

Management: FCS_CKM_EXT.4

There are no management activities foreseen.

Audit: FCS_CKM_EXT.4

There are no audit events foreseen.

5.2.1.1 FCS_CKM_EXT.4 - Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

Rationale

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.2.2 Extended: IPsec selected (FCS_IPSEC)

Family behaviour

This family addresses requirements for protecting communications using IPsec.

Component levelling

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management: FCS_IPSEC_EXT.1

There are no management activities foreseen.

Audit: FCS_IPSEC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Failure to establish an IPsec SA.

5.2.2.1 FCS_IPSEC_EXT.1 - Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1 Cryptographic key generation
FCS_COP.1 Cryptographic operation
FCS_RBG_EXT.1 Extended: Random Bit Generation

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: **tunnel mode, transport mode**].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: **the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106**].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: **IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers] and [selection: no other RFCs for hash functions, RFC 4868 for hash functions], IKEv2 as defined in RFCs 5996 [selection: with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23] and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]**].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: **IKEv1, IKEv2**] protocol uses the cryptographic algorithms AES-CBC-128, Protection Profile for Hardcopy Devices – v1.0 September 10, 2015 Page 112 AES-CBC-256 as specified in RFC 3602 and [selection: **AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm**].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: **IKEv2 SA lifetimes can be established based on [selection: number of packets/number of bytes, length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs], IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes, length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]**].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: **24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)), [assignment: other DH groups that are implemented by the TOE], no other DH groups**].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: **RSA, ECDSA**] algorithm and Pre-shared Keys

Rationale

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.2.3 Extended: Cryptographic Operation (Key Chaining) (FCS_KYC)

Family behaviour

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

Component levelling

FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

Management: FCS_KYC_EXT.1

There are no management activities foreseen.

Audit: FCS_KYC_EXT.1

There are no audit events foreseen.

5.2.3.1 FCS_KYC_EXT.1 - Extended: Key Chaining

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(E) No description found, or
FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation, or
FCS_SMC_EXT.1 No description found]

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: **one, using a submask as the BEV or DEK, intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): [selection: key transport as specified in FCS_COP.1(i)]**] while maintaining an effective strength of [selection: **128 bits, 256 bits**].

Rationale

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.

This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.2.4 Extended: 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.

5.2.4.1 FCS_RBG_EXT.1 - Extended: 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 [selection: **ISO/IEC 18031:2011, 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 [selection: **[assignment: number of software-based sources] software-based noise source(s), [assignment: number of hardware-based sources] hardware-based noise source(s)**] with a minimum of [selection: **128 bits, 256 bits**] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security strength table for hash functions", 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.

5.3 Class FDP: User data protection

5.3.1 Extended: Protection of Data on Disk (FDP_DSK)

Family behaviour

This family is to mandate the encryption of all protected data written to the storage.

Component levelling

FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

Management: FDP_DSK_EXT.1

There are no management activities foreseen.

Audit: FDP_DSK_EXT.1

There are no audit events foreseen.

5.3.1.1 FDP_DSK_EXT.1 - Extended: Protection of Data on Disk

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FDP_DSK_EXT.1.1 The TSF shall be [selection: **perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP**] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

Rationale

Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.4 Class FIA: Identification and authentication

5.4.1 Extended: Password Management (FIA_PMG)

Family behaviour

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component levelling

FIA_PMG _EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

There are no management activities foreseen.

Audit: FIA_PMG_EXT.1

There are no audit events foreseen.

5.4.1.1 FIA_PMG_EXT.1 - Extended: Password Management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters [selection: **"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"**]
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

Rationale

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.4.2 Extended: Pre-Shared Key Composition (FIA_PSK)

Family behaviour

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

Component levelling

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates

Management: FIA_PSK_EXT.1

There are no management activities foreseen.

Audit: FIA_PSK_EXT.1

There are no audit events foreseen.

5.4.2.1 FIA_PSK_EXT.1 - Extended: Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Random Bit Generation

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [selection: **[assignment: other supported lengths], no other lengths**]
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: **SHA-1, SHA2-256, SHA2-512, [assignment: method of conditioning text string]**] and be able to [selection: **use no other pre-shared keys, accept bit-based pre-shared keys, generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1**].

Rationale

Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.5 Class FPT: Protection of the TSF

5.5.1 Extended: Protection of Key and Key Material (FPT_KYP)

Family behaviour

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

Component levelling

FPT_ KYP _EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management: FPT_KYP_EXT.1

There are no management activities foreseen.

Audit: FPT_KYP_EXT.1

There are no audit events foreseen.

5.5.1.1 FPT_KYP_EXT.1 - Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such plaintext key on a device that uses the key for its encryption.

Rationale

Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.5.2 Extended: Protection of TSF Data (FPT_SKP)

Family behaviour

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

Component levelling

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

There are no audit events foreseen.

5.5.2.1 FPT_SKP_EXT.1 - Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Rationale

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.5.3 Extended: TSF Testing (FPT_TST)

Family behaviour

This family addresses the requirements for self-testing the TSF for selected correct.

Component levelling

FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1

There are no management activities foreseen.

Audit: FPT_TST_EXT.1

There are no audit events foreseen.

5.5.3.1 FPT_TST_EXT.1 - Extended: TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Rationale

TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.5.4 Extended: Trusted Update (FPT_TUD)

Family behaviour

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component levelling

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

Management: FPT_TUD_EXT.1

There are no management activities foreseen.

Audit: FPT_TUD_EXT.1

There are no audit events foreseen.

5.5.4.1 FPT_TUD_EXT.1 - Extended: Trusted Update

Hierarchical to: No other components.

Dependencies: [FCS_COP.1 Cryptographic operation]

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [**published hash, no other functions**] prior to installing those updates.

Rationale

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 1: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		HCDPP	No	No	Yes	No
	FAU_GEN.2 User identity association		HCDPP	No	No	No	No
	FAU_STG_EXT.1 Extended: Audit Trail Storage		HCDPP	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1(a) Cryptographic key generation (for asymmetric keys)	FCS_CKM.1	HCDPP	Yes	No	No	Yes
	FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)	FCS_CKM.1	HCDPP	Yes	Yes	No	Yes
	FCS_CKM_EXT.4 Extended: Cryptographic key material destruction		HCDPP	No	No	No	No
	FCS_CKM.4 Cryptographic key destruction		HCDPP	No	No	No	Yes
	FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)	FCS_COP.1	HCDPP	Yes	No	Yes	Yes
	FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)	FCS_COP.1	HCDPP	Yes	No	Yes	Yes
	FCS_COP.1(c) Cryptographic operation (Hash algorithm)	FCS_COP.1	HCDPP	Yes	Yes	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_COP.1(g) Cryptographic operation (for keyed-hash message authentication)	FCS_COP.1	HCDPP	Yes	Yes	Yes	Yes
	FCS_IPSEC_EXT.1 Extended: IPsec selected		HCDPP	No	No	Yes	Yes
	FCS_KYC_EXT.1 Extended: Key chaining		HCDPP	No	No	No	Yes
	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)		HCDPP	No	Yes	Yes	Yes
FDP - User data protection	FDP_ACC.1 Subset access control		HCDPP	No	No	No	No
	FDP_ACF.1 Security attribute based access control		HCDPP	No	No	Yes	No
	FDP_DSK_EXT.1 Extended: Protection of Data on Disk		HCDPP	No	No	No	Yes
	FDP_RIP.1(a) Subset residual information protection	FDP_RIP.1	HCDPP	Yes	No	No	No
FIA - Identification and authentication	FIA_AFL.1 Authentication failure handling		HCDPP	No	No	Yes	Yes
	FIA_ATD.1 User attribute definition		HCDPP	No	No	Yes	No
	FIA_PMG_EXT.1 Extended: Password Management		HCDPP	No	Yes	Yes	Yes
	FIA_PSK_EXT.1 Extended: Pre-shared key composition		HCDPP	No	Yes	Yes	Yes
	FIA_UAU.1 Timing of authentication		HCDPP	No	No	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FIA_UAU.7 Protected authentication feedback		HCDPP	No	No	Yes	No
	FIA_UID.1 Timing of identification		HCDPP	No	No	Yes	No
	FIA_USB.1 User-subject binding		HCDPP	No	No	Yes	No
FMT - Security management	FMT_MOF.1 Management of security functions behaviour		HCDPP	No	Yes	Yes	Yes
	FMT_MSA.1 Management of security attributes		HCDPP	No	No	Yes	Yes
	FMT_MSA.3 Static attribute initialisation		HCDPP	No	Yes	Yes	Yes
	FMT_MTD.1 Management of TSF data		HCDPP	No	No	Yes	Yes
	FMT_SMF.1 Specification of Management Functions		HCDPP	No	No	Yes	No
	FMT_SMR.1 Security roles		HCDPP	No	No	No	No
FPT - Protection of the TSF	FPT_KYP_EXT.1 Extended: Protection of Key and Material		HCDPP	No	No	No	No
	FPT_SKP_EXT.1 Extended: Protection of TSF data		HCDPP	No	No	No	No
	FPT_STM.1 Reliable time stamps		HCDPP	No	No	No	No
	FPT_TST_EXT.1 Extended: TSF testing		HCDPP	No	No	No	No
	FPT_TUD_EXT.1 Extended: Trusted Update		HCDPP	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FTA - TOE access	FTA_SSL.3 TSF-initiated termination		HCDPP	No	No	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		HCDPP	No	No	Yes	Yes
	FTP_TRP.1(a) Trusted path (for Administrators)	FTP_TRP.1	HCDPP	Yes	No	No	Yes

Table 12: SFRs for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

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

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

c) All auditable events specified in Table 13, **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, additional information specified in Table 13, **none**.

Auditable events	Relevant SFR	Additional information	Origin
Job completion	FDP_ACF.1	Type of job	[HCDPP]
Unsuccessful user authentication	FIA_UAU.1	Required by [HCDPP]: • None Added by vendor: • For unsuccessful remote user authentication, the origin of attempt	[HCDPP]

		(e.g., IP address)	
Unsuccessful user identification	FIA_UID.1	Required by [HCDPP]: • None Added by vendor: • The attempted user identity • For unsuccessful remote user identification, the origin of attempt (e.g., IP address)	[HCDPP]
Use of management functions	FMT_SMF.1	None	[HCDPP]
Modification to the group of Users that are part of a role	FMT_SMR.1	None	[HCDPP]
Changes to the time	FPT_STM.1	Required by [HCDPP]: • None Added by vendor: • New date and time • Old date and time	[HCDPP]
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a)	Required by [HCDPP]: • Reason for failure Added by vendor: • Non-TOE endpoint of connection (e.g., IP address)	[HCDPP]
Locking an account	FIA_AFL.1	User name associated with account	Vendor
Unlocking an account	FIA_AFL.1	User name associated with account	Vendor

Table 13: Auditable Events

TSS Link: TSS for FAU_GEN.1.

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.

TSS Link: TSS for FAU_GEN.2.

6.1.1.3 Extended: Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

TSS Link: TSS for FAU_STG_EXT.1.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (for asymmetric keys) (FCS_CKM.1(a))

FCS_CKM.1.1(a) The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with

- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes**
- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and P-521 (as defined in FIPS PUB 186-4, "Digital Signature Standard")**

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

Usage	Implementation	Purpose	Algorithm	Key sizes	Related SFRs
IPsec	HP FutureSmart QuickSec 5.1	KAS FFC	DH (dhEphem)	P=2048, SHA2-256	FCS_COP.1(c), FCS_IPSEC_EXT.1, FCS_RBG_EXT.1
			DSA	L=2048, N=224; L=2048, N=256; L=3072, N=256	

		KAS ECC	ECDH (ephemeral unified)	P-256, SHA2-256; P-384, SHA2-384; P-521, SHA2-512	
			ECDSA	P-256, P-384, P-521	

Table 14: Asymmetric key generation

TSS Link: TSS for FCS_CKM.1(a).

6.1.2.2 Cryptographic key generation (Symmetric Keys) (FCS_CKM.1(b))

FCS_CKM.1.1(b) The TSF shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes ***defined in Table 15*** that meet the following: No Standard.

Usage	Implementation	Purpose	Key sizes	Related SFRs
Drive-lock password (BEV)	HP FutureSmart OpenSSL FIPS Object Module 2.0.4	BEV generation	256 bit	FCS_KYC_EXT.1, FCS_RBG_EXT.1

Table 15: Symmetric key generation

TSS Link: TSS for FCS_CKM.1(b).

6.1.2.3 Extended: Cryptographic key material destruction (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

TSS Link: TSS for FCS_CKM_EXT.4.

6.1.2.4 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- **For volatile memory, the destruction shall be executed by a removal of power to the memory;**

that meets the following: No Standard.

TSS Link: TSS for FCS_CKM.4.

6.1.2.5 Cryptographic Operation (Symmetric encryption/decryption) (FCS_COP.1(a))

FCS_COP.1.1(a) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in **the modes defined in Table 16** and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- **NIST SP 800-38A**

Usage	Implementation	Purpose	Algo-rithm	Modes	Key sizes	Related SFRs
IPsec	HP FutureSmart QuickSec 5.1	Data encryption and decryption	AES	CBC	128 bits, 256 bits	FCS_IPSEC_EXT.1
		Encryption in CTR_DRBG(AES)	AES	ECB	256 bits	
Drive-lock password (BEV)	HP FutureSmart OpenSSL FIPS Object Module 2.0.4	AES encryption in CTR_DRBG(AES)	AES	CTR	256 bits	FCS_KYC_EXT.1, FCS_RBG_EXT.1
			AES	ECB	256 bits	

Table 16: AES encryption/decryption algorithms

TSS Link: TSS for FCS_COP.1(a).

6.1.2.6 Cryptographic Operation (for signature generation/verification) (FCS_COP.1(b))

FCS_COP.1.1(b) The TSF shall perform cryptographic signature services in accordance with a

- **RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of the bit sizes defined in Table 17**

that meets the following
Case: RSA Digital Signature Algorithm

- **FIPS PUB 186-4, "Digital Signature Standard".**

Usage	Implementation	Purpose	Algorithm	Key sizes	Related SFR
IPsec	HP FutureSmart QuickSec 5.1	Signature generation and verification based on PKCS#1 v1.5	RSA	2048 bits, 3072 bits	FCS_IPSEC_EXT.1
Trusted update	HP FutureSmart Rebex Total Pack 2017 R1	Signature verification based on PKCS#1 v1.5	RSA	2048 bits	FPT_TUD_EXT.1
TSF testing	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	Signature verification based on PKCS#1 v1.5	RSA	2048 bits	FPT_TST_EXT.1

Table 17: Asymmetric algorithms for signature generation/verification

TSS Link: TSS for FCS_COP.1(b).

6.1.2.7 Cryptographic operation (Hash algorithm) (FCS_COP.1(c))

FCS_COP.1.1(c) The TSF shall perform cryptographic hashing services in accordance with **the algorithms in Table 18** that meet the following: [ISO/IEC 10118-3:2004].

Usage	Implementation	Purpose	Algorithms	Related SFR
IPsec	HP FutureSmart QuickSec 5.1	Pre-shared keys	***SHA-1, SHA2-256, SHA2-512***	FIA_PSK_EXT.1
		KAS FFC	***SHA2-256***	FCS_CKM.1(a)
		KAS ECC	***SHA2-256, SHA2-384, SHA2-512***	
		RSA digital signature generation	***SHA2-256, SHA2-384, SHA2-512***	FCS_COP.1(b)
		RSA digital signature verification	***SHA-1, SHA2-256, SHA2-384, SHA2-512***	

		HMAC	***SHA-1, SHA2-256, SHA2-384, SHA2-512***	FCS_COP.1(g)
Trusted update	HP FutureSmart Rebex Total Pack 2017 R1	RSA digital signature verification	***SHA2-256***	FPT_TUD_EXT.1
TSF testing	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	RSA digital signature verification	***SHA2-256***	FPT_TST_EXT.1

Table 18: Hash algorithms

TSS Link: TSS for FCS_COP.1(c).

6.1.2.8 Cryptographic operation (for keyed-hash message authentication) (FCS_COP.1(g))

FCS_COP.1.1(g) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm ~~HMAC~~ ***defined in Table 19***, key size ***defined in Table 19*** and message digest sizes ***defined in Table 19*** in bits that meet the following: FIPS PUB 198-1, 'The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."'

Usage	Implementation	Algorithm	Key size	Digest size	Related SFR
IPsec	HP FutureSmart QuickSec 5.1	HMAC-SHA-1	160 bits	160 bits	FCS_IPSEC_EXT.1
		HMAC-SHA2-256	256 bits	256 bits	
		HMAC-SHA2-384	384 bits	384 bits	
		HMAC-SHA2-512	512 bits	512 bits	

Table 19: HMAC algorithms

TSS Link: TSS for FCS_COP.1(g).

6.1.2.9 Extended: IPsec selected (FCS_IPSEC_EXT.1)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement **transport mode**.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using **the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC**.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: **IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, no other RFCs for extended sequence numbers and RFC 4868 for hash functions** .

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the **IKEv1** protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and **no other algorithm**.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that **IKEv1 SA lifetimes can be established based on length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs**.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and **DH Group 15 (3072-bit MODP), DH Group 16 (4096-bit MODP), DH Group 17 (6144-bit MODP), DH Group 18 (8192-bit MODP)**.

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the **RSA** algorithm and Pre-shared Keys.

TSS Link: TSS for FCS_IPSEC_EXT.1.

6.1.2.10 Extended: Key chaining (FCS_KYC_EXT.1)

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: **one, using submasks as the BEV or DEK** while maintaining an effective strength of **256 bits**.

TSS Link: TSS for FCS_KYC_EXT.1.

6.1.2.11 Extended: Cryptographic Operation (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 ***the algorithm defined in Table 20***.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **the number defined in Table 20 of hardware-based noise source(s)** with a minimum of ***bits defined in Table 20*** of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

Usage	Implementation	Algorithm	Hardware noise sources	Minimum entropy bits	Related SFRs
IPsec	HP FutureSmart QuickSec 5.1	CTR_DRBG(AES)	1	256 bits	FCS_CKM.1(a), FCS_COP.1(a), FCS_IPSEC_EXT.1
Drive-lock password (BEV)	HP FutureSmart OpenSSL FIPS Object Module 2.0.4	CTR_DRBG(AES)	1	256 bits	FCS_CKM.1(b), FCS_COP.1(a), FCS_KYC_EXT.1

Table 20: DRBG algorithms

TSS Link: TSS for FCS_RBG_EXT.1.

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the User Data Access Control SFP on subjects, objects, and operations among subjects and objects specified in Table 21 and Table 22.

TSS Link: TSS for FDP_ACC.1.

6.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the User Data Access Control SFP to objects based on the following: subjects, objects, and attributes specified in Table 21 and Table 22.

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 governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 21 and Table 22.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

		"Create"	"Read"	"Modify"	"Delete"
Scan	*Operation:*	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	**allowed**	**allowed**	**denied by design**	**allowed**
	U.ADMIN	**denied**	**denied**	**denied**	**allowed**
	U.NORMAL	**denied**	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied

Table 21: D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Scan	*Operation:*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	**allowed** (note 1)	**allowed**	**denied by design**	**allowed**
	U.ADMIN	**denied**	**allowed**	**denied by design**	**allowed**
	U.NORMAL	**denied**	Status: **allowed** Log: **denied**	denied	denied
	Unauthenticated	denied	Status: **allowed** Log: **denied**	denied	denied

Table 22: D.USER.JOB Access Control SFP

TSS Link: TSS for FDP_ACF.1.

Note 1: Job Owner is assigned to an authorized User as part of the process of initiating a scan Job.

6.1.3.3 Extended: Protection of Data on Disk (FDP_DSK_EXT.1)

FDP_DSK_EXT.1.1 The TSF shall **use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP**, such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

TSS Link: TSS for FDP_DSK_EXT.1.

6.1.3.4 Subset residual information protection (FDP_RIP.1(a))

FDP_RIP.1.1(a) The TSF shall ensure that any previous information content of a resource is made unavailable by overwriting data upon the deallocation of the resource from the following objects: D.USER.DOC.

TSS Link: TSS for FDP_RIP.1(a).

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **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, EWS, and RESTful**
    - **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**.

TSS Link: TSS for FIA_AFL.1.

6.1.4.2 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**
    - **Internal Authentication (Local Device Sign In)**
        - **Identifier: Display name**
        - **Authenticator: Password**

        - **PS: Device Administrator PS**
    - **External Authentication (LDAP Sign In and Windows Sign In)**
        - **PS: Network user PS**
- **EWS users**
    - **Internal Authentication (Local Device Sign In)**
        - **Identifier: Display name**
        - **Authenticator: Password**
        - **Role: (implied U.ADMIN)**
    - **External Authentication (LDAP Sign In and Windows Sign In)**
        - **Role: (implied U.ADMIN)**
- **RESTful users**
    - **Internal Authentication (Local Device Sign In)**
        - **Identifier: Display name**
        - **Authenticator: Password**
        - **Role: (implied U.ADMIN)**
    - **External Authentication (Windows Sign In)**
        - **Role: (implied U.ADMIN)**

TSS Link: TSS for FIA_ATD.1.

6.1.4.3 Extended: Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters

- *Device Administrator Password*
    - **"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "", "'", "`", "+", ",", "-", ".", "/", "\", ":", ";", "<", "=", ">", "?", "[", "]", "_", "|", "~", "{", "}"**

b) Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

TSS Link: TSS for FIA_PMG_EXT.1.

Application Note: This SFR applies to the Device Administrator Password which is used by the Control Panel, EWS, and RESTful interfaces.

6.1.4.4 Extended: Pre-shared key composition (FIA_PSK_EXT.1)

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

a) 22 characters in length and **up to 128 characters in length**;

b) composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using **SHA-1, SHA2-256, SHA2-512** and be able to **accept bit-based pre-shared keys**.

TSS Link: TSS for FIA_PSK_EXT.1.

6.1.4.5 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

- **Control Panel:**
  - **Viewing of Welcome message**
  - **Resetting of Control Panel**
  - **Selection of Sign In**
  - **Selection of sign-in method from Sign In screen**
  - **Viewing of device status information**
  - **Changing display language for the session**
  - **Viewing of network connectivity status information**
  - **Viewing of help information**
  - **Viewing of system time**
- **EWS:**
  - **Selection of sign in method**
- **RESTful:**

- **No TSF-mediated actions**

on behalf of the user to be performed before the user is authenticated.

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

TSS Link: TSS for FIA_UAU.1.

6.1.4.6 Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **dots** to the user while the authentication is in progress.

TSS Link: TSS for FIA_UAU.7.

6.1.4.7 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

- **Control Panel:**
  - **Viewing of Welcome message**
  - **Resetting of Control Panel**
  - **Selection of Sign In**
  - **Selection of sign-in method from Sign In screen**
  - **Viewing of device status information**
  - **Changing display language for the session**
  - **Viewing of network connectivity status information**
  - **Viewing of help information**
  - **Viewing of system time**
- **EWS:**
  - **Selection of sign in method**
- **RESTful:**
  - **No TSF-mediated actions**

on behalf of the user to be performed before the user is identified.

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

TSS Link: TSS for FIA_UID.1.

6.1.4.8 User-subject binding (FIA_USB.1)

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

1) **User identifier**
    - **Control Panel users:**
        - **Local Device Sign In method: Display name**
        - **LDAP Sign In method: LDAP username**
        - **Windows Sign In method: Windows username**
    - **EWS users:**
        - **Local Device Sign In: Display name**
        - **LDAP Sign In: LDAP username**
        - **Windows Sign In: Windows username**
    - **RESTful users:**
        - **Local Device Sign In: Display name**
        - **Windows Sign In: Windows username**
2) **User role**
    - **Control Panel users: U.ADMIN and U.NORMAL (User session PS)**
    - **EWS users: U.ADMIN**
    - **RESTful users: U.ADMIN**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **Control Panel and EWS user session PS:**

- **Internal Authentication (Local Device Sign In)**
    - **Device Administrator session PS = Device Administrator PS**
- **External Authentication (LDAP Sign In and Windows Sign In)**

- If a PS is associated with a network user account, then: **User session PS = Network user PS + Device Guest PS**
- Else, if the network user is associated with one or more network group PSs, then: **User session PS = Network group PSs + Device Guest PS**
- Else: **User session PS = External Authentication method PS + Device Guest PS**

- **If the "Allow users to choose alternate sign-in methods" function is disabled, the user's session PS calculated above 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 subjects acting on the behalf of users:

- **None—The TOE does not allow a subject to change its in-session security attributes.**

.

TSS Link: TSS for FIA_USB.1.

6.1.5 Security management (FMT)

6.1.5.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform the actions defined in Table 23 on*** the functions **defined in Table 23** to U.ADMIN.

Function	Actions	Related SFRs	Application note
Allow users to choose alternate sign-in methods at the product control panel	Enable, disable	FIA_USB.1	The “Allow users to choose alternate sign-in methods at the product control panel” function affects how the TOE authorizes Control Panel users.
Control Panel full authentication	Enable, disable	FIA_ATD.1, FIA_UAU.1, FIA_UID.1	In the evaluated configuration, the "Control Panel Full Authentication" function must be enabled.
Windows Sign In	Enable, disable		In the evaluated configuration, at least one External Authentication mechanism (Windows Sign In or LDAP Sign In) must be enabled.

LDAP Sign In	Enable, disable		In the evaluated configuration, at least one External Authentication mechanism (Windows Sign In or LDAP Sign In) must be enabled.
Account lockout	Enable, disable	FIA_AFL.1	In the evaluated configuration, account lockout for Device Administrator account must be enabled.
Enhanced security event logging	Enable, disable	FAU_GEN.1	In the evaluated configuration, enhanced security event logging must be enabled.
Managing Temporary Job Files (i.e., image overwrite)	Determine the behavior of, modify the behavior of	FDP_RIP.1(a)	The TOE offers three options: Non-Secure Fast Erase (no overwrite), Secure Fast Erase (overwrite 1 time), and Secure Sanitize Erase (overwrite 3 times). In the evaluated configuration, the administrator must select either Secure Fast Erase or Secure Sanitize Erase.
IPsec	Enable, disable	FCS_IPSEC_EXT.1	In the evaluated configuration, IPsec must be enabled.
Automatically synchronize with a Network Time Service	Enable, disable	FPT_STM.1	In the evaluated configuration, NTS must be enabled.

Table 23: Management of function

TSS Link: TSS for FMT_MOF.1.

6.1.5.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the User Data Access Control SFP to restrict the ability to **perform the restricted operations defined in Table 24 on** the security attributes **defined in Table 24** to **the authorized identified roles defined in Table 24**.

TOE component	Security attribute	Available operations	Restricted operations	Authorized identified roles	Default value property	Default value override roles
Control Panel and EWS subject attributes	Account identity (Internal Authentication mechanism)	None	None	n/a	n/a	No role

	Account identity (External Authentication mechanisms)	None	None	n/a	n/a	No role
	Device Administrator permission set permissions	View	View	U.ADMIN	Permissive	No role
	Device User and Device Guest permission set permissions	Modify, view	Modify, view	U.ADMIN	Restrictive	No role
	Custom permission set permissions	Create, modify, delete, view	Create, modify, delete, view	U.ADMIN	Restrictive	No role

Table 24: Management of function

TSS Link: TSS for FMT_MSA.1.

6.1.5.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the User Data Access Control SFP to provide **the properties defined in Table 24 of the** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***default value override role defined in Table 24*** specify alternative initial values to override the default values when an object or information is created.

TSS Link: TSS for FMT_MSA.3.

HCDPP Application Note: FMT_MSA.3.2 applies only to security attributes whose default values can be overridden.

6.1.5.4 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability **to perform the specified operations on the specified TSF Data to the roles specified in** Table 25 .

Data	Operation	Authorized roles	Related SFR(s)
List of TSF Data owned by U.NORMAL or associated with Documents or jobs owned by a U.NORMAL			
None	**n/a**	**n/a**	**n/a**

List of TSF Data not owned by U.NORMAL			
Device Administrator password	**Change**	U.ADMIN	FIA_PMG_EXT.1
Permission set associations (except on the Device Administrator account)	**Add, change, delete, view**	U.ADMIN	FDP_ACF.1, FMT_MSA.1
Permission set associations (only on the Device Administrator account)	**View**	U.ADMIN	
List of software, firmware, and related configuration data			
IPsec CA and identity certificates	**Import, delete**	U.ADMIN	FCS_IPSEC_EXT.1
IPsec pre-shared keys	**Set, change**	U.ADMIN	FIA_PSK_EXT.1
Internal clock settings	**Change**	U.ADMIN	FPT_STM.1
NTS server configuration data	**Change**	U.ADMIN	
Minimum password length	**Change**	U.ADMIN	FIA_PMG_EXT.1
Account lockout maximum attempts	**Change**	U.ADMIN	FIA_AFL.1
Account lockout interval	**Change**	U.ADMIN	
Account reset lockout counter interval	**Change**	U.ADMIN	
Session inactivity timeout	**Change**	U.ADMIN	FTA_SSL.3

Table 25: Management of TSF Data

TSS Link: TSS for FMT_MTD.1.

6.1.5.5 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **defined in Table 26**.

Management function	SFR	TSS page number	Objectives
Management of Device Administrator password	FMT_MTD.1	130	O.USER_AUTHORIZATION, O.USER_I&A
Management of account lockout policy	FMT_MTD.1	130	O.USER_I&A
Management of minimum length password settings	FMT_MTD.1	130	
Management of Internal and External authentication mechanisms	FMT_MOF.1	127	
Management of "Allow users to choose alternate sign-in methods at the product control panel" function	FMT_MOF.1	127	
Management of session inactivity timeouts	FMT_MTD.1	130	
Management of permission set associations	FMT_MTD.1	130	O.ADMIN_ROLES
Management of permission set permissions	FMT_MSA.1	128	O.ACCESS_CONTROL
Management of IPsec pre-shared keys	FMT_MTD.1	130	O.COMMS_PROTECTION
Management of CA and identity certificates for IPsec authentication	FMT_MTD.1	130	
Management of enhanced security event logging	FMT_MOF.1	127	O.AUDIT
Management of internal clock settings	FMT_MTD.1	130	
Management of NTS configuration data	FMT_MTD.1	130	
Management of image overwrite option in "Managing Temporary Job Files"	FMT_MOF.1	127	O.IMAGE_OVERWRITE

Table 26: Specification of management functions

TSS Link: TSS for FMT_SMF.1.

6.1.5.6 Security roles (FMT_SMR.1)

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

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

TSS Link: TSS for FMT_SMR.1.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Extended: Protection of Key and Material (FPT_KYP_EXT.1)

FPT_KYP_EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device.

TSS Link: TSS for FPT_KYP_EXT.1.

6.1.6.2 Extended: Protection of TSF data (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

TSS Link: TSS for FPT_SKP_EXT.1.

HCDPP Application Note: The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through "normal" interfaces. While it is understood that the administrator could directly read memory to view these keys, doing so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not engage in such an activity.

6.1.6.3 Reliable time stamps (FPT_STM.1)

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

TSS Link: TSS for FPT_STM.1.

6.1.6.4 Extended: TSF testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

TSS Link: TSS for FPT_TST_EXT.1.

6.1.6.5 Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and **no other functions** prior to installing those updates.

TSS Link: TSS for FPT_TUD_EXT.1.

Application Note: The HP Inc. Software Depot kiosk provides a SHA2-256 published hash of the update image and a Windows OS utility program that can be downloaded and used to verify the hash. Once downloaded, the update image can be verified on a separate computer prior to installation on the TOE using the published hash and the Windows OS utility program. Because the published hash verification is not performed by the TSF, the SHA2-256 published hash verification method is excluded from this SFR.

6.1.7 TOE access (FTA)

6.1.7.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **administrator-configurable amount of time of user inactivity**.

TSS Link: TSS for FTA_SSL.3.

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 use **IPsec** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **authentication server, DNS server, FTP server, NTS server, SharePoint server, SMB server, SMTP server, syslog server, and WINS server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities, to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **authentication server, DNS server, FTP server, NTS server, SharePoint server, SMB server, SMTP server, syslog server, and WINS server**.

TSS Link: TSS for FTP_ITC.1.

6.1.8.2 Trusted path (for Administrators) (FTP_TRP.1(a))

FTP_TRP.1.1(a) The TSF shall use **IPsec** to provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2(a) The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3(a) The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

TSS Link: TSS for FTP_TRP.1(a).

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

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

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FAU_STG_EXT.1	O.AUDIT
FCS_CKM.1(a)	O.COMMS_PROTECTION
FCS_CKM.1(b)	O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION
FCS_CKM_EXT.4	O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION
FCS_CKM.4	O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION
FCS_COP.1(a)	O.COMMS_PROTECTION
FCS_COP.1(b)	O.COMMS_PROTECTION, O.UPDATE_VERIFICATION

Security functional requirements	Objectives
FCS_COP.1(c)	O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.UPDATE_VERIFICATION
FCS_COP.1(g)	O.COMMS_PROTECTION
FCS_IPSEC_EXT.1	O.COMMS_PROTECTION
FCS_KYC_EXT.1	O.STORAGE_ENCRYPTION
FCS_RBG_EXT.1	O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION
FDP_ACC.1	O.ACCESS_CONTROL, O.USER_AUTHORIZATION
FDP_ACF.1	O.ACCESS_CONTROL, O.USER_AUTHORIZATION
FDP_DSK_EXT.1	O.STORAGE_ENCRYPTION
FDP_RIP.1(a)	O.IMAGE_OVERWRITE
FIA_AFL.1	O.USER_I&A
FIA_ATD.1	O.USER_AUTHORIZATION
FIA_PMG_EXT.1	O.USER_I&A
FIA_PSK_EXT.1	O.COMMS_PROTECTION
FIA_UAU.1	O.USER_I&A
FIA_UAU.7	O.USER_I&A
FIA_UID.1	O.ADMIN_ROLES, O.USER_I&A
FIA_USB.1	O.USER_I&A
FMT_MOF.1	O.ADMIN_ROLES

Security functional requirements	Objectives
FMT_MSA.1	O.ACCESS_CONTROL, O.USER_AUTHORIZATION
FMT_MSA.3	O.ACCESS_CONTROL, O.USER_AUTHORIZATION
FMT_MTD.1	O.ACCESS_CONTROL
FMT_SMF.1	O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION
FMT_SMR.1	O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION
FPT_KYP_EXT.1	O.KEY_MATERIAL
FPT_SKP_EXT.1	O.COMMS_PROTECTION
FPT_STM.1	O.AUDIT
FPT_TST_EXT.1	O.TSF_SELF_TEST
FPT_TUD_EXT.1	O.UPDATE_VERIFICATION
FTA_SSL.3	O.USER_I&A
FTP_ITC.1	O.AUDIT, O.COMMS_PROTECTION
FTP_TRP.1(a)	O.COMMS_PROTECTION

Table 27: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

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

Security objectives	Rationale
O.USER_I&A	

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td></td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FIA_AFL.1</td><td>Supports</td><td>This SFR protects the authentication function by limiting the number of unauthorized authentication attempts that can be made, thereby reducing the likelihood of impersonation.</td></tr>
<tr><td>FIA_PMG_EXT.1</td><td>Satisfies</td><td>This SFR protects the authentication function by providing for strong credentials that are difficult to guess or derive.</td></tr>
<tr><td>FIA_UAU.1</td><td>Satisfies</td><td>This SFR defines the TOE functions that can be performed without authentication and the functions that require authentication for use.</td></tr>
<tr><td>FIA_UAU.7</td><td>Satisfies</td><td>This SFR protects the authentication function by hiding the authentication credential as it is being input.</td></tr>
<tr><td>FIA_UID.1</td><td>Satisfies</td><td>This SFR defines the TOE functions that can be performed without identification and the functions that require identification for use.</td></tr>
<tr><td>FIA_USB.1</td><td>Satisfies</td><td>This requirement provides assurance that an identified user is associated with attributes that govern their authorizations to the TSF upon successful authentication to the TOE.</td></tr>
<tr><td>FTA_SSL.3</td><td>Satisfies</td><td>This SFR helps prevent User or Administrator impersonation by terminating unattended sessions.</td></tr>
</table>
</td></tr>
<tr><td>O.ACCESS_CONTROL</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FDP_ACC.1</td><td>Satisfies</td><td>This SFR defines the access control policy that is used to protect access to User Data and TSF Data.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Security objectives</th><th colspan="3">Rationale</th></tr>
<tr><td></td><td>FDP_ACF.1</td><td>Satisfies</td><td>This SFR defines the specific rule-set that constitutes the access control policy, identifying the conditions under which access to resources, functions, and data are authorized or denied."</td></tr>
<tr><td></td><td>FMT_MSA.1</td><td>Supports</td><td rowspan="5">The management of the product configuration, security settings, and user attributes and authorizations is critical to maintaining operational security. These management functions, as a group, provide for the ability of authorized administrators to configure the system, add and delete users, grant user-specific authorizations to system data, resources, and functions, introduce code (e.g., updates) into the system, and assign users to roles. Additionally, the SFRs also require that management functions be limited to users who have been explicitly authorized to perform management functions.</td></tr>
<tr><td></td><td>FMT_MSA.3</td><td>Supports</td></tr>
<tr><td></td><td>FMT_MTD.1</td><td>Supports</td></tr>
<tr><td></td><td>FMT_SMF.1</td><td>Supports</td></tr>
<tr><td></td><td>FMT_SMR.1</td><td>Supports</td></tr>
<tr><td>O.USER_AUTHORIZATION</td><td colspan="3"><table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FDP_ACC.1</td><td>Supports</td><td>This SFR enforces User Access Control SFP on subjects, objects, and operations in accordance with user authorization.</td></tr>
<tr><td>FDP_ACF.1</td><td>Supports</td><td>This SFR enforces the User Access Control SFP to objects based on attributes in accordance with user authorization.</td></tr>
<tr><td>FIA_ATD.1</td><td>Supports</td><td>This SFR defines the attributes that are associated with Users that can be used to define their authorizations.</td></tr>
<tr><td>FMT_MSA.1</td><td>Satisfies</td><td>This SFR defines the authorizations that are required to access data that is protected by the TSF.</td></tr>
<tr><td>FMT_MSA.3</td><td>Satisfies</td><td>This SFR defines the default security posture for enforcement of the access control policy that governs access to data that is protected by the TSF.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td></td><td>
<table>
<tr><td>FMT_SMF.1</td><td>Satisfies</td><td>This SFR defines the management functions provided by the TOE that can be used to define User authorizations.</td></tr>
<tr><td>FMT_SMR.1</td><td>Satisfies</td><td>This SFR defines administrative roles that can be used to define authorizations to groups of Users.</td></tr>
</table>
</td></tr>
<tr><td>O.ADMIN_ROLES</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FIA_UID.1</td><td>Supports</td><td>This SFR defines the TOE management functions that can be accessed without requiring Administrator authorization.</td></tr>
<tr><td>FMT_MOF.1</td><td>Satisfies</td><td>This SFR defines the authorizations that are required for Administrators to access TOE functions.</td></tr>
<tr><td>FMT_SMF.1</td><td>Satisfies</td><td>This SFR defines the administrative functions that are provided by the TSF.</td></tr>
<tr><td>FMT_SMR.1</td><td>Satisfies</td><td>This SFR defines the different roles that can be assigned to Administrators for the purposes of determining authentication and authorization.</td></tr>
</table>
</td></tr>
<tr><td>O.UPDATE_VERIFICATION</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FCS_COP.1(b)</td><td>Selection</td><td>This SFR defines the digital signature service(s) used to verify the authenticity TOE updates.</td></tr>
<tr><td>FCS_COP.1(c)</td><td>Selection</td><td>This SFR defines the hashing algorithm(s) used to verify the integrity of TOE updates.</td></tr>
<tr><td>FPT_TUD_EXT.1</td><td>Satisfies</td><td>This SFR defines the ability of the TOE to be updated and the method(s) by which the updates are known to be trusted.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td>O.TSF_SELF_TEST</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FPT_TST_EXT.1</td><td>Satisfies</td><td>This SFR defines the ability of the TSF to perform self-tests which assert the security properties of the TOE.</td></tr>
</table>
</td></tr>
<tr><td>O.COMMS_PROTECTION</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FCS_CKM.1(a)</td><td>Satisfies</td><td>This SFR defines the use of secure algorithms for key pair generation that can be used for key transport during protected communications.</td></tr>
<tr><td>FCS_CKM.1(b)</td><td>Satisfies</td><td>This SFR defines the use of secure algorithms for key generation that can be used for protection communications.</td></tr>
<tr><td>FCS_CKM.4</td><td>Supports</td><td>This SFR defines the method of data erasure used by FCS_CKM_EXT.4 that provides assurance that cryptographic keys that need to be erased cannot be recovered.</td></tr>
<tr><td>FCS_CKM_EXT.4</td><td>Supports</td><td>This SFR ensures that residual cryptographic data cannot be used to compromise protected communications.</td></tr>
<tr><td>FCS_COP.1(a)</td><td>Satisfies</td><td>This SFR defines the use of a secure symmetric key algorithm that can be used for protected communications.</td></tr>
<tr><td>FCS_COP.1(b)</td><td>Satisfies</td><td>This SFR defines the digital signature services(s) used for protected communications.</td></tr>
<tr><td>FCS_COP.1(c)</td><td>Selection</td><td>This mapping is missing from [HCDPP] Table 17. This SFR defines the hashing algorithm(s) used to condition the IPsec text-based, pre-shared keys.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td></td><td>
<table>
<tr><td>FCS_COP.1(g)</td><td>Satisfies</td><td>This SFR defines the use of a secure HMAC algorithm that can be used for protected communications.</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>Selection</td><td>This SFR defines secure communications protocols that can be used to protect the transmission of security-relevant data.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>Supports</td><td>This SFR supports protected communications by defining a secure method of random bit generation that allows cryptographic functions to operate with their theoretical maximum strengths.</td></tr>
<tr><td>FIA_PSK_EXT.1</td><td>Selection</td><td>This SFR defines the use of pre-shared keys in IPsec which allows for the secure implementation of that protocol.</td></tr>
<tr><td>FPT_SKP_EXT.1</td><td>Satisfies</td><td>This SFR prevents the compromise of protected communications by ensuring that secret cryptographic data is protected against unauthorized access.</td></tr>
<tr><td>FTP_ITC.1</td><td>Satisfies</td><td>This SFR defines the interfaces over which protected communications are required and the methods used to protect the communications used to transit those interfaces.</td></tr>
<tr><td>FTP_TRP.1(a)</td><td>Satisfies</td><td>This SFR defines the protected communications path that is used to secure Administrator interaction with the TOE.</td></tr>
</table>
</td></tr>
<tr><td>O.AUDIT</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FAU_GEN.1</td><td>Satisfies</td><td>This SFR defines the auditable events for which the TOE generates audit data and the fields that are included in each audit record.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td></td><td>
<table>
<tr><td>FAU_GEN.2</td><td>Satisfies</td><td>This SFR defines the ability of the TOE to apply attribution to all activities performed by a user or Administrator.</td></tr>
<tr><td>FAU_STG_EXT.1</td><td>Satisfies</td><td>This SFR defines the ability of the TSF to transmit generated audit data to an external entity using a protected channel.</td></tr>
<tr><td>FPT_STM.1</td><td>Supports</td><td>This SFR ensures that audit data is labeled with accurate timestamps.</td></tr>
<tr><td>FTP_ITC.1</td><td>Supports</td><td>This SFR defines the protected communications channel(s) over which audit data can be transmitted.</td></tr>
</table>
</td></tr>
<tr><td>O.STORAGE_ENCRYPTION</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FCS_CKM.1(b)</td><td>Selection</td><td>This SFR defines the use of secure algorithms for key generation that can be used for storage encryption.</td></tr>
<tr><td>FCS_CKM_EXT.4</td><td>Supports</td><td>This SFR helps define the requirements for the proper destruction of cryptographic keys in order to ensure that stored data is unrecoverable should the storage device(s) be separated from the TOE.</td></tr>
<tr><td>FCS_COP.1(c)</td><td>Not supported</td><td>This PP dependency is not implemented by the TOE. Instead, the TOE uses an SED as the field-replaceable, nonvolatile storage device to fulfill this requirement.</td></tr>
<tr><td>FCS_KYC_EXT.1</td><td>Satisfies</td><td>This SFR defines the key chaining method used by the TOE to provide multiple layers of security for key material.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Security objectives</th><th>Rationale</th></tr>
<tr><td></td><td>
<table>
<tr><td>FCS_RBG_EXT.1</td><td>Supports</td><td>This SFR defines the random bit generation algorithm used to ensure that the TOE's cryptographic algorithms function with the theoretical maximum level of security.</td></tr>
<tr><td>FDP_DSK_EXT.1</td><td>Satisfies</td><td>This SFR requires the TSF to encrypt the data that is stored to disk.</td></tr>
</table>
</td></tr>
<tr><td>O.KEY_MATERIAL</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FPT_KYP_EXT.1</td><td>Satisfies</td><td>This SFR defines the ability of the TSF from storing unprotected key data in insecure locations.</td></tr>
</table>
</td></tr>
<tr><td>O.IMAGE_OVERWRITE</td><td>
<table>
<tr><th>SFR</th><th>Relationship</th><th>Rationale</th></tr>
<tr><td>FDP_RIP.1(a)</td><td>Satisfies</td><td>This SFR defines the ability of the TSF to overwrite user document data upon its deallocation.</td></tr>
</table>
</td></tr>
</table>

Table 28: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of the SFRs modeled in CC Part 2, [HCDPP] and [HCDPP-ERRATA], and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1

Security functional requirement	Dependencies	Resolution
	FTP_ITC.1	FTP_ITC.1
FCS_CKM.1(a)	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1(b) resolves, but FCS_COP.1(i) is excluded from the ST. See Section 6.2.4 for exclusion rationale.
	FCS_CKM.4	This dependency has been removed by the PP.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_CKM.1(b)	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1(a) FCS_COP.1(g)
	FCS_CKM.4	This dependency has been removed by the PP.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_CKM_EXT.4	FCS_CKM.1	FCS_CKM.1(a) FCS_CKM.1(b)
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(a) FCS_CKM.1(b)
FCS_COP.1(a)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(b)
	FCS_CKM.4	This dependency has been removed by the PP.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4

Security functional requirement	Dependencies	Resolution
FCS_COP.1(b)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved because RSA keys are imported by the TOE via X.509v3 certificates, not generated by the TOE. FCS_CKM.1(a) is for the generation of DH and DSA keys.
	FCS_CKM.4	This dependency has been removed by the PP.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_COP.1(c)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency has been removed by the PP.
	FCS_CKM.4	This dependency has been removed by the PP.
FCS_COP.1(g)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(b)
	FCS_CKM.4	This dependency has been removed by the PP.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_IPSEC_EXT.1	FCS_CKM.1	FCS_CKM.1(a)
	FCS_COP.1	FCS_COP.1(a) FCS_COP.1(b) FCS_COP.1(c) FCS_COP.1(g)
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
	FIA_PSK_EXT.1	FIA_PSK_EXT.1
FCS_KYC_EXT.1	FCS_COP.1	FCS_COP.1(e), FCS_COP.1(f), and FCS_COP.1(i) are excluded from the ST. See Section 6.2.4 for exclusion rationale.

Security functional requirement	Dependencies	Resolution
	FCS_KDF_EXT.1	FCS_KDF_EXT.1 is excluded from the ST. See Section 6.2.4 for exclusion rationale.
	FCS_SMC_EXT.1	FCS_SMC_EXT.1 is excluded from the ST. See Section 6.2.4 for exclusion rationale.
FCS_RBG_EXT.1	No dependencies	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3
FDP_DSK_EXT.1	FCS_COP.1	FCS_COP.1(d) is excluded from the ST. See Section 6.2.4 for exclusion rationale.
FDP_RIP.1(a)	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_PMG_EXT.1	No dependencies	
FIA_PSK_EXT.1	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1

Security functional requirement	Dependencies	Resolution
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
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_KYP_EXT.1	No dependencies	
FPT_SKP_EXT.1	No dependencies	
FPT_STM.1	No dependencies	
FPT_TST_EXT.1	No dependencies	

Security functional requirement	Dependencies	Resolution
FPT_TUD_EXT.1	FCS_COP.1	FCS_COP.1(b) FCS_COP.1(c)
FTA_SSL.3	No dependencies	
FTP_ITC.1	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1
FTP_TRP.1(a)	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1

Table 29: TOE SFR dependency analysis

6.2.4 HCDPP SFR reconciliation

This ST excludes the follow SFRs found in [HCDPP].

Excluded PP SFR	Type	Rationale
FAU_SAR.1	Optional	Optional
FAU_SAR.2	Optional	Optional
FAU_STG.1	Optional	Optional
FAU_STG.4	Optional	Optional
FCS_COP.1(d)	Selection-based	O.STORAGE_ENCRYPTION: FCS_COP.1(d) is for AES data encryption and decryption of stored data on field-replaceable, nonvolatile storage devices by the TOE. The TOE does not perform AES data encryption and decryption of stored data on field-replaceable, nonvolatile storage devices. Instead, the TOE uses an SED for data encryption and decryption. The SED perform its own data encryption and decryption.
FCS_COP.1(e)	Selection-based	O.STORAGE_ENCRYPTION: FCS_COP.1(e) is defined in [HCDPP] for key wrapping within the key chain. The TOE does not use key wrapping in the key chain; thus, key wrapping is not selected in FCS_KYC_EXT.1.

Excluded PP SFR	Type	Rationale
FCS_COP.1(f)	Selection-based	O.STORAGE_ENCRYPTION: FCS_COP.1(f) is defined in [HCDPP] for AES encryption of keys in the key chain. The TOE does not use symmetric encryption algorithms to encrypt keys in the key chain; thus, AES key encryption is not selected in FCS_KYC_EXT.1.
FCS_COP.1(h)	Selection-based	O.STORAGE_ENCRYPTION: FCS_COP.1(h) is defined in [HCDPP] for keyed-hash message authentication algorithms for creating the BEV. The TOE does not use HMACs to create the BEV.
FCS_COP.1(i)	Selection-based	O.STORAGE_ENCRYPTION: FCS_COP.1(i) is defined in [HCDPP] for key transport encryption within the key chain. The TOE does not use key transport encryption in the key chain; thus, key transport is not selected in FCS_KYC_EXT.1.
FCS_HTTPS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1.
FCS_KDF_EXT.1	Selection-based	O.STORAGE_ENCRYPTION: FCS_KDF_EXT.1 is defined in [HCDPP] for generating intermediate keys. The TOE does not generate or use intermediate keys related to O.STORAGE_ENCRYPTION.
FCS_PCC_EXT.1	Selection-based	O.STORAGE_ENCRYPTION: FCS_PCC_EXT.1 is defined in [HCDPP] for cryptographic password construction and conditioning of the BEV. The TOE generates the BEV from the RBG instead of from a password.
FCS_SMC_EXT.1	Selection-based	O.STORAGE_ENCRYPTION: FCS_SMC_EXT.1 is defined in [HCDPP] for submask combining. The TOE does not use submask combining in the key chain; thus, submask combining is not selected in FCS_KYC_EXT.1.
FCS_SNI_EXT.1	Selection-based	O.STORAGE_ENCRYPTION: FCS_SNI_EXT.1 is defined in [HCDPP] for generation of salts, nonces, and initialization vectors when manual entry of a drive encryption passphrase is supported by the TOE. The TOE does not support manual entry of a drive encryption passphrase.
FCS_SSH_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_TLS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.

Excluded PP SFR	Type	Rationale
FDP_RIP.1(b)	Optional	O.PURGE_DATA is not supported in the evaluated configuration.
FTP_TRP.1(b)	Conditionally Mandatory	The TOE is a scan-only device that does not have a remote, non-administrative interface.
FDP_FXS_EXT.1	Conditionally Mandatory	The TOE does not have PSTN faxing capabilities.

Table 30: HCDPP SFRs excluded from the ST

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE correspond to the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.

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

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ASE Security Target evaluation	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_OBJ.1 Security objectives for the operational environment	CC Part 3	No	No	No	No
	ASE_REQ.1 Stated security requirements	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ADV Development	ADV_FSP.1 Basic functional specification	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
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.1 Labelling of the TOE	CC Part 3	No	No	No	No
	ALC_CMS.1 TOE CM coverage	CC Part 3	No	No	No	No
ATE Tests	ATE_IND.1 Independent testing - conformance	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.1 Vulnerability survey	CC Part 3	No	No	No	No

Table 31: SARs

6.4 Security Assurance Requirements Rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the PP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.

7 TOE Summary Specification

7.1 TOE Security Functionality

The TSS page numbers in Table 32 provide a quick index to each SFR's TSS entry in Table 33 of the next section.

Table 32: TSS Index

SFR	TSS page		SFR	TSS page		SFR	TSS page		SFR	TSS page
FAU_GEN.1	89		FCS_IPSEC_EXT.1	108		FIA_PSK_EXT.1	120		FPT_KYP_EXT.1	134
FAU_GEN.2	95		FCS_KYC_EXT.1	112		FIA_UAU.1	120		FPT_SKP_EXT.1	135
FAU_STG_EXT.1	96		FCS_RBG_EXT.1	113		FIA_UAU.7	124		FPT_STM.1	135
FCS_CKM.1(a)	97		FDP_ACC.1	114		FIA_UID.1	124		FPT_TST_EXT.1	136
FCS_CKM.1(b)	99		FDP_ACF.1	114		FIA_USB.1	125		FPT_TUD_EXT.1	136
FCS_CKM_EXT.4	99		FDP_DSK_EXT.1	115		FMT_MOF.1	127		FTA_SSL.3	137
FCS_CKM.4	100					FMT_MSA.1	128		FTP_ITC.1	138
FCS_COP.1(a)	102		FDP_RIP.1(a)	116		FMT_MSA.3	130		FTP_TRP.1(a)	139
FCS_COP.1(b)	103		FIA_AFL.1	117		FMT_MTD.1	130			
FCS_COP.1(c)	104		FIA_ATD.1	118		FMT_SMF.1	132			
FCS_COP.1(g)	107		FIA_PMG_EXT.1	119		FMT_SMR.1	133			

The list of CAVP certificates is in Section 7.1.2 on page 140. The CAVP certificates are also listed with each SFR description in the following section.

7.1.1 TOE SFR compliance rationale

Table 33 provides the rationale for how the TOE complies with each of the SFRs in Section 6.1. Table 33 uses the following abbreviations.

- AA—Assurance Activity
- n/a—Not applicable
- Op env—Operational environment for CAVP certificates

- Resp—Response

Table 33: TOE SFR compliance rationale

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td>FAU_GEN.1
(Audit generation)</td><td>
<table>
<tr><td>Objective(s):</td><td>O.AUDIT</td></tr>
</table>
<u>Summary</u>
The TOE generates audit records for the audit events specified in [HCDPP]. It also generates audit records for additional vendor-specific audit events defined in FAU_GEN.1.

To generate the proper set of audit events, the TOE's enhanced security event logging must be enabled. For information on this, see the TSS for FMT_MOF.1.

The complete audit record format and audit record details are provided in the [CCECG] section Security event logging messages. The [CCECG] groups the events into event categories in the subsection Log messages.

Table 34 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.)

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.

Table 34: TOE audit records
<table>
<tr><th>Required event</th><th>Additional information</th><th>[CCECG] "Log messages" category and records</th><th>Comments</th></tr>
<tr><td>Audit start-up</td><td>None</td><td><u>Security event logging</u>
Records:
1) Auditing was started during boot up
2) Auditing was restarted using EWS</td><td></td></tr>
<tr><td>Audit shutdown</td><td>None</td><td><u>Security event logging</u>
Record:
1) Auditing was stopped using EWS</td><td></td></tr>
<tr><td>Job completion</td><td>Type of job</td><td><u>Job completion</u>
Records:
1) Email job completion (Scan to Email)</td><td></td></tr>
</table>
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale			
			2) Save (scan) to Sharepoint job completion 3) Save (scan) to Network Folder job completion 4) Email job completion	
	Unsuccessful user authentication	[HCDPP]: • None Vendor: • For unsuccessful remote user authentication, the origin of attempt (e.g., IP address)	<u>Local device sign in</u> Record: 1) Local Device sign-in method failed for the specified user	
			<u>Windows sign in</u> Record: 1) Windows sign in method failed for the specified user	
			<u>LDAP sign in</u> Record: 1) LDAP sign in method failed for the specified user	
	Unsuccessful user identification	[HCDPP]: • None Vendor: • Attempted user identity • For unsuccessful remote user identification, the origin of attempt (e.g., IP address)	Same events as the "Unsuccessful user authentication" events	
	Use of management functions FMT_SMF.1	None	<u>Management of Device Administrator password</u> Record: 1) Device administrator password modified	

TOE SFRs	TOE SFR compliance rationale					
				Management of account lockout policy Records: 1) Account Lockout Policy enabled 2) Account Lockout Policy disabled 3) Account Lockout Policy setting modified		
				Management of minimum length password settings Record: 1) Minimum Password Length Policy setting modified		
				Management of Internal and External authentication mechanisms Records: 1) LDAP Sign In enabled 2) LDAP Sign In disabled 3) LDAP Sign In configuration modified 4) Windows Sign In enabled 5) Windows Sign In disabled 6) Windows Sign In configuration modified		
				Management of "Allow users to choose alternate sign-in methods at the product control panel" function Record: 1) Sign In and Permission Policy settings modified		
				Management of session inactivity timeouts Records:		

TOE SFRs	TOE SFR compliance rationale				
				1) Control Panel Inactivity Timeout Changed 2) EWS Session Timeout modified	
				<u>Management of permission set associations</u> Records: 1) Default Permission Set for sign-in method modified 2) Group to Permission Set Relationship added 3) Group to Permission Set Relationship deleted 4) User to Permission Set Relationship added 5) User to Permission Set Relationship deleted	
				<u>Management of permission set permissions</u> Records: 1) Permission Set added 2) Permission Set copied 3) Permission Set deleted 4) Permission Set modified	
				<u>Management of IPsec pre-shared keys</u> Records: 1) IPsec policy added 2) IPsec policy deleted 3) IPsec policy modified	
				<u>Management of CA and identity certificates for IPsec authentication</u> Records: 1) Device CA certificate installed	

TOE SFRs	TOE SFR compliance rationale				
				2) Device CA certificate deleted 3) Device Identity certificate and private key installed 4) Device Identity certificate deleted	
				Management of enhanced security event logging Records: 1) CCC logging started 2) CCC logging stopped	
				Management of internal clock settings Records: 1) System time changed 2) Date and Time configuration modified	
				Management of NTS configuration data Record: 1) Date and Time configuration modified	
				Management of image overwrite option in "Managing Temporary Job Files" Record: 1) File Erase Mode for erasing temporary job files modified	
		Modification to the group of users that are part of a role	None	Network user to permission set relationships Records: 1) User to permission set relationship added via EWS	

TOE SFRs	TOE SFR compliance rationale				
				2) User to permission set relationship deleted via EWS 3) User to permission set relationship added via EWS 4) User to permission set relationship deleted via EWS	
				Network group to permission set relationships Records: 1) Group to permission set relationship added via EWS 2) Group to permission set relationship deleted via EWS 3) Group to permission set relationship added via EWS 4) Group to permission set relationship deleted via EWS	
		Changes to the time	[HCDPP]: • None Vendor: • New date and time • Old date and time	System time Records: 1) Changed at the control panel 2) Changed via EWS 3) Changed by NTS 4) Changed settings/attributes (e.g., DST, TZ)	
		Failure to establish session (trusted channel/path)	[HCDPP]: • Reason for failure	IKEv1 phase 1 negotiations Records: 1) IKEv1 phase 1 negotiation failed initiated by the client computer	Reason: IKEv1 phase 1 negotiation failed

<table>
<tr><th>TOE SFRs</th><th colspan="4">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><td></td><td>Vendor:

• Non-TOE endpoint of connection (e.g. IP address)</td><td>2) IKEv1 phase 1 negotiation failed initiated by the local device (TOE)</td><td></td></tr>
<tr><td></td><td></td><td><u>IKEv1 phase 2 negotiations</u>
Records:
1) IKEv1 phase 2 negotiation failed initiated by the client computer
2) IKEv1 phase 2 negotiation failed initiated by the local device (TOE)</td><td>Reason: IKEv1 phase 2 negotiation failed</td></tr>
<tr><td>Locking an account</td><td>User name associated with account</td><td><u>Account Entered Lockout Mode</u>
Records:
1) Account Lockout Mode was entered for the Local Administrator account</td><td></td></tr>
<tr><td>Unlocking an account</td><td>User name associated with account</td><td><u>Account Exited Lockout Mode</u>
Records:
1) Account Lockout Mode was exited for Local Administrator account</td><td></td></tr>
</table></td></tr>
<tr><td></td><td>AA</td><td colspan="3">The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its recorded information are consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td colspan="3">Table 13 contains the auditable events for FAU_GEN.1. Table 34 contains the TSS auditable events and records.</td></tr>
<tr><td>FAU_GEN.2 (Audit user identification)</td><td colspan="4"><table>
<tr><td>Objective(s):</td><td>O.AUDIT</td></tr>
</table><u>Summary</u>
Events resulting from actions of identified users are associated with the identity of the user that caused the event.</td></tr>
<tr><td></td><td>AA</td><td colspan="3">The Assurance Activities for FAU_GEN.1 address this SFR.</td></tr>
<tr><td></td><td>Resp</td><td colspan="3">n/a</td></tr>
<tr><td></td><td colspan="4"></td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td>FAU_STG_EXT.1 (Audit trail storage)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.AUDIT</td></tr>
</table>
<u>Summary</u>
The TOE connects and sends audit records to an external syslog server for long-term storage and audit review. It uses the syslog protocol to transmit the records over an IPsec channel. The IPsec channel provides protection of the transmitted data and assured identification of both endpoints.

The TOE contains two in-memory audit record message queues. One queue is for network audit records (e.g., IPsec records) generated and maintained by the Jetdirect Inside Firmware and the other queue is for HCD audit records (e.g., Control Panel Sign In events) generated and maintained by the System firmware. These in-memory message queues are not accessible through any TOE interface and, thus, are protected against unauthorized access.

The network queue holds up to 15 audit records. New audit records are discarded when the network queue becomes full. The HCD queue holds up to 1000 audit records. New audit records replace the oldest audit records when the HCD queue becomes full.

The TOE establishes a persistent connection to the external syslog server. An audit record is generated, added to a queue, immediately sent from the queue to the syslog server, and then removed from the queue once the record has been successfully received by the syslog server.

If the connection is interrupted (e.g., network outage), the TOE will make 5 attempts to reestablish the connection where each attempt lasts for approximately 30 seconds. If all attempts fail, the TOE will repeat the reestablishment process again when a new audit record is added to the HCD queue. Once the connection is reestablished, the records from both queues are immediately sent to the syslog server.

If the TOE is powered off, any audit records remaining in the two in-memory messages queues at the time of power-off will be discarded.

Note: The TOE also stores up to 500 audit records on the SED replacing the oldest audit records with new audit records, but these records are not accessible through any external interface in the evaluated configuration and, thus, are protected against unauthorized access.
<table>
<tr><td>AA</td><td>The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.</td></tr>
<tr><td>Resp</td><td>The TOE uses the syslog protocol over an IPsec channel to transfer audit data to the external audit server.</td></tr>
<tr><td>AA</td><td>The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>There are two in-memory audit record message queues: network queue and HCD queue. The network queue holds up to 15 records and, if full, discards new records. The HCD queue holds up to 1000 records and, if full, replaces the oldest records with new records. When an audit record is added to a queue, it is immediately sent to the external syslog server (assuming a connection to the server exists). Once a record is sent, it is removed from the queue. No TOE interface is provided to access these queues, thus, no unauthorized access is possible.</td></tr>
<tr><td>FCS_CKM.1(a) (Asymmetric key generation)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
For IPsec IKEv1 KAS FFC, the TOE uses the DH key pair generation algorithm to establish a protected communication channel. A portion of the DH key generation algorithm is the same as the DSA key generation algorithm. Because of this, the CAVP testing for DH contains a prerequisite for testing the DSA key generation function used by the DH key generation function. Thus, DSA key generation is a prerequisite for and included as part of KAS FFC.

For IPsec IKEv1 KAS ECC, the TOE uses the ECDH key pair generation algorithm to establish a protected communication channel. A portion of the ECDH key generation algorithm is the same as the ECDSA key generation algorithm. Because of this, the CAVP testing for ECDH contains a prerequisite for testing the ECDSA key generation function used by the ECDH key generation function. Thus, ECDSA key generation is a prerequisite for and included as part of KAS FFC.

For KAS FFC, the TOE uses the DH ephemeral (dhEphem) scheme with SHA2-256 for key establishment as per the NIST Special Publication (SP) [SP800-56A-Rev3] standard Section 5.5.1.1 "FFC Domain Parameter Generation" tests FB and FC, Section 5.6.1.1 "FFC Key-Pair Generation," and Section 6.1.2.1 "dhEphem, C(2e, 0s, FFC DH) Scheme." The DH/DSA key pair generation supports the following values as per the [FIPS186-4] standard.
• L=2048, N=224
• L=2048, N=256
• L=3072, N=256

For KAS ECC, the TOE uses the ECDH ephemeral unified scheme with the following curve and SHA algorithm combinations for key establishment as per the NIST SP [SP800-56A-Rev3] standard Section 5.5.1.2 "ECC Domain Parameter Generation" tests EC, ED, and EE, Section 5.6.1.2 "ECC Key-Pair Generation," and Section 6.1.2.2 "(Cofactor) Ephemeral Unified Model, C(2e, 0s, ECC CDH)."
• EC: P-256, SHA2-256
• ED: P-384, SHA2-384
• EE: P-521, SHA2-512

The ECDH/ECDSA key pair generation supports the P-256, P-384, and P-521 curves as per the [FIPS186-4] standard.
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale

For both KAS FFC and KAS ECC, any necessary key material is obtained using the QuickSec 5.1 CTR_DRBG(AES) defined in FCS_RBG_EXT.1.

The TOE uses the HP FutureSmart QuickSec 5.1 for all IPsec cryptography.

The TOE does not implement the key derivation function (KDF) defined in the NIST SP [SP800-56A-Rev3] standard. Instead, the TOE implements the IPsec IKEv1 KDF. The IKEv1 KDF was not tested through the CAVP as CAVP testing of this KDF was considered optional by NIAP at the time of this evaluation.

The TOE uses RSA-based X.509v3 certificates for IPsec/IKEv1 authentication using the IPsec IKEv1 digital signature authentication method. (See FCS_COP.1(b) for RSA digital signature generation and verification.) The TOE does **not** perform RSA key pair generation. Instead, the RSA certificates are generated by the Operational Environment and imported by the TOE. Therefore, RSA key pair generation is not claimed in FCS_CKM.1(a).

Table 35: Asymmetric key generation

Usage	Implementation	Op env	Algorithm	Modes & key sizes	CAVP cert #
IPsec	HP FutureSmart QuickSec 5.1	Arm Cortex-A8	DH (dhEphem)	SHA2-256	CVL #1999
			DSA	L=2048, N=224; L=2048, N=256; L=3072, N=256	DSA #1432
			ECDH (ephemeral unified)	EC: P-256, SHA2-256; ED: P-384, SHA2-384; EE: P-521, SHA2-512	CVL #1999
			ECDSA	P-256, P-384, P-521	ECDSA #1501

Table 46 contains the complete list of cryptographic operations and CAVP certificates.

AA	*The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.*

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>The Summary section above provides the explanation.</td></tr>
<tr><td></td><td>AA</td><td>Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS. The TSS may refer to the Key Management Description (KMD), described in [HCDPP] Appendix F, that may not be made available to the public.</td></tr>
<tr><td></td><td>Resp</td><td>There are no TOE-specific extensions. As mentioned in the Summary section, the KDF used by the TOE is the IKEv1 KDF.</td></tr>
<tr><td>FCS_CKM.1(b) (Symmetric key generation)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.STORAGE_ENCRYPTION</td></tr>
</table>
<u>Summary</u>
The TOE uses the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 CTR_DRBG(AES) defined in FCS_RBG_EXT.1 to generate the key used for the SED's drive-lock password (BEV). Table 36 shows the purpose and key sizes generated and the standards to which they conform. For information on how the TOE invokes the DRBG, see the [KMD].
Table 36: Symmetric key generation
<table>
<tr><th>Usage</th><th>Implementation</th><th>Purpose</th><th>Op env</th><th>Key size</th><th>Standard</th></tr>
<tr><td>Drive-lock password (BEV)</td><td>HP FutureSmart OpenSSL FIPS Object Module 2.0.4</td><td>BEV generation</td><td>Arm Cortex-A8</td><td>256-bit</td><td>No standard</td></tr>
</table>
</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.</td></tr>
<tr><td></td><td>Resp</td><td>This information is provided in the [KMD].</td></tr>
<tr><td>FCS_CKM_EXT.4 (Key material destruction)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.STORAGE_ENCRYPTION</td></tr>
</table>
<u>Summary</u>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">The TOE's plaintext secret and private cryptographic keys and cryptographic critical security parameters (CSPs) are as follows.

• IPsec keys and key material (for O.COMMS_PROTECTION)

• Drive-lock password (for O.STORAGE_ENCRYPTION)

TSS for FCS_CKM.4 contains an accounting of the keys and key material, when these values are no longer needed, and when to expect them to be destroyed.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.</td></tr>
<tr><td></td><td>Resp</td><td>The TSS for FCS_CKM.4 contains the requested information on a per key basis.</td></tr>
<tr><td>FCS_CKM.4
(Key destruction)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.STORAGE_ENCRYPTION</td></tr>
</table>
<u>Summary</u>
As stated in the TSS for FCS_CKM_EXT.4, the TOE's plaintext secret and private cryptographic keys and cryptographic critical security parameters (CSPs) are as follows.

• IPsec keys and key material (for O.COMMS_PROTECTION)

• SED drive-lock password (for O.STORAGE_ENCRYPTION)

Table 37 contains the list of the IPsec volatile memory keys, their usage, their storage location, when they are no longer needed, when they are destroyed, and their destruction algorithm.

<u>Rationale for no nonvolatile key destruction</u>

Although the following keys reside in nonvolatile memory, the nonvolatile selection in the [HCDPP] FCS_CKM.4 is not selected because of the following reasons.

• Drive-lock password (BEV)—This plaintext secret used to unlock the SED(s) is generated once by the TOE in the evaluated configuration, stored in non-field replaceable nonvolatile memory (EEPROM), is always needed, is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified in the evaluated configuration, thus, it is never destroyed.

• IPsec Pre-shared keys—The PSKs are stored on the SED and, thus, are considered to be stored as ciphertext, not plaintext.

• IPsec RSA private key—This private key is stored on the SED and, thus, is considered to be stored as ciphertext, not plaintext.</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale

Table 37: TOE key destruction

Secret type	Usage	Storage location	No longer needed	When destroyed	Destruction algorithm
IPsec Diffie-Hellman (DH) private exponent	The private exponent used in DH exchange (generated by the TOE)	RAM	After DH shared secret generation	Power off	Power loss
IPsec DH shared secret	Shared secret generated by the DH key exchange (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec SKEYID	Value derived from the shared secret within IKE exchange (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec IKE session encrypt key	The IKE session encrypt key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec IKE session authentication key	The IKE session authentication key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec pre-shared key	The key used to generate the IKE SKEYID during pre-shared key authentication (entered by the administrator)	RAM	After SKEYID generation	Power off	Power loss
IPsec IKE RSA private key	RSA private key for IKE authentication	RAM	After session establishment	Power off	Power loss
IPsec encryption key	The IPsec encryption key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec authentication key	The IPsec authentication key	RAM	Session termination	Power off	Power loss
Drive-lock password (BEV)	The SED password. Generated by the TOE.	RAM	After boot	Power off	Power loss

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>AA</td><td>The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.</td></tr>
<tr><td></td><td>Resp</td><td>The Summary section above contains the requested information on a per key basis.</td></tr>
<tr><td>FCS_COP.1(a) (AES)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
IPsec supports both AES CBC 128-bit and AES CBC 256-bit for symmetric data encryption and decryption and AES ECB 256-bit for the symmetric encryption in CTR_DRBG(AES) using the HP FutureSmart QuickSec 5.1 meeting both [FIPS197] and [SP800-38A] standards.

The drive-lock password generation supports AES CTR 256-bit (which, for CAVP testing, has a dependency on AES ECB 256-bit) for symmetric encryption in CTR_DRBG(AES) using the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 meeting both [FIPS197] and [SP800-38A] standards.

Table 38: AES algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Op env</th><th>Algorithm</th><th>Modes & key sizes</th><th>CAVP cert #</th></tr>
<tr><td rowspan="2">IPsec</td><td rowspan="2">HP FutureSmart QuickSec 5.1</td><td rowspan="2">Arm Cortex-A8</td><td>AES encryption and decryption</td><td>AES-CBC-128, AES-CBC-256</td><td rowspan="2">AES #5567</td></tr>
<tr><td>AES encryption</td><td>AES-ECB-256</td></tr>
<tr><td rowspan="2">Drive-lock password (BEV)</td><td rowspan="2">HP FutureSmart OpenSSL FIPS Object Module 2.0.4</td><td rowspan="2">Arm Cortex-A8</td><td>AES encryption</td><td>AES-CTR-256</td><td rowspan="2">AES #5563</td></tr>
<tr><td>AES encryption</td><td>AES-ECB-256</td></tr>
</table>
Table 46 contains the complete list of cryptographic operations and CAVP certificates.
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>AA</td><td>None</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FCS_COP.1(b) (RSA)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.UPDATE_VERIFICATION</td></tr>
</table>
<u>Summary</u>
The TOE's IPsec uses RSA certificates for digital signature-based authentication. IPsec uses the RSA 2048-bit and 3072-bit algorithms for digital signature authentication (i.e., signature generation and verification) using the HP FutureSmart QuickSec 5.1. The RSA signature generation is based on PKCS#1 v1.5 and uses SHA2-256, SHA2-384, and SHA2-512. The RSA signature verification is based on PKCS#1 v1.5 and uses SHA-1, SHA2-256, SHA2-384, and SHA2-512. For more details on IPsec, see the TSS for FCS_IPSEC_EXT.1.

The TOE's trusted update function uses the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 for digital signature verification. This function uses the HP FutureSmart Rebex Total Pack 2017 R1 implementation of the RSA 2048-bit algorithm. For more details on trusted update, see the TSS for FPT_TUD_EXT.1.

The TOE's TSF testing (Whitelisting) function uses the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 for digital signature verification. This function uses the HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation of the RSA 2048-bit algorithm. For more details on TSF testing, see the TSS for FPT_TST_EXT.1.

All implementations meet the [FIPS186-4] standard.

Table 39: Asymmetric algorithms for signature generation/verification
<table>
<tr><th>Usage</th><th>Implementation</th><th>Op env</th><th>Algorithm</th><th>Key sizes</th><th>CAVP cert #</th></tr>
<tr><td>IPsec</td><td>HP FutureSmart QuickSec 5.1</td><td>Arm Cortex-A8</td><td>RSA signature generation based on PKCS#1 v1.5 using SHA2-256, SHA2-384, SHA2-512</td><td>2048-bits, 3072-bits</td><td>RSA #2996</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>RSA signature verification based on PKCS#1 v1.5 using SHA-1, SHA2-256, SHA2-384, SHA2-512</td><td>2048-bits, 3072-bits</td><td>RSA #2996</td></tr>
<tr><td>Trusted update</td><td>HP FutureSmart Rebex Total Pack 2017 R1</td><td>Arm Cortex-A8</td><td>RSA signature verification based on PKCS#1 v1.5 using SHA2-256</td><td>2048-bits</td><td>RSA #2993</td></tr>
<tr><td>TSF testing</td><td>HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937</td><td>Arm Cortex-A8</td><td>RSA signature verification based on PKCS#1 v1.5 using SHA2-256</td><td>2048-bits</td><td>RSA #2994</td></tr>
</table>
Table 46 contains the complete list of cryptographic operations and CAVP certificates.
<table>
<tr><td>AA</td><td>None</td></tr>
<tr><td>Resp</td><td>n/a</td></tr>
</table>
</td></tr>
<tr><td>FCS_COP.1(c) (SHS)</td><td>
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.UPDATE_VERIFICATION</td></tr>
<tr><td></td><td>O.STORAGE_ENCRYPTION— The TOE uses an SED as the field-replaceable, nonvolatile storage device to fulfill this requirement; therefore, the TOE does not implement FCS_COP.1(c) for this objective. For more information on the SED, see FDP_DSK_EXT.1 and the TSS for FDP_DSK_EXT.1.</td></tr>
</table>
<u>Summary</u>
<u>IPsec</u>
IPsec supports the conditioning of text-based, pre-shared keys using SHA-1, SHA2-256, and SHA2-512 hash algorithms as specified in FIA_PSK_EXT.1.
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
IPsec supports SHA2-256 for KAS FFC and SHA2-256, SHA2-384, and SHA2-512 for KAS ECC as specified in FCS_CKM.1(a).

IPsec supports SHA2-256, SHA2-384, and SHA2-512 for RSA signature generation and SHA-1, SHA2-256, SHA2-384, and SHA2-512 for RSA signature verification as specified in FCS_COP.1(b).

Also, IPsec supports HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 which use SHA-1, SHA2-256, SHA2-384, and SHA2-512, respectively.

IPsec uses the HP FutureSmart QuickSec 5.1 implementation for these algorithms. For more details on pre-shared keys, see the TSS for FIA_PSK_EXT.1. For more details on signature generation and verification, see the TSS for FCS_COP.1(b). For more details on the HMAC algorithms, see the TSS for FCS_COP.1(g).

Trusted update

The TOE's trusted update function uses the SHA2-256 algorithm for RSA digital signature verification. This function uses the HP FutureSmart Rebex Total Pack 2017 R1 implementation of the SHA2-256 algorithm. For more details on trusted update, see the TSS for FPT_TUD_EXT.1.

TSF testing

The TOE's TSF testing (Whitelisting) function uses the SHA2-256 algorithm for RSA digital signature verification. This function uses the HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation of the SHA2-256 algorithm. For more details on TSF testing, see the TSS for FPT_TST_EXT.1.

All implementations meet the [ISO-10118-3] standard.

Table 40: SHS algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Op env</th><th>Purpose</th><th>Modes & key sizes</th><th>CAVP cert #</th></tr>
<tr><td rowspan="3">IPsec</td><td rowspan="3">HP FutureSmart QuickSec 5.1</td><td rowspan="3">Arm Cortex-A8</td><td>Pre-shared keys</td><td>SHA-1, SHA2-256, SHA2-512</td><td rowspan="3">SHS #4474</td></tr>
<tr><td>KAS FFC</td><td>SHA2-256</td></tr>
<tr><td>KAS ECC</td><td>SHA2-256, SHA2-384, SHA2-512</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale						
					RSA digital signature generation	SHA2-256, SHA2-384, SHA2-512	
					RSA digital signature verification	SHA-1, SHA2-256, SHA2-384, SHA2-512	
					HMAC	SHA-1, SHA2-256, SHA2-384, SHA2-512	
		Trusted update	HP FutureSmart Rebex Total Pack 2017 R1	Arm Cortex-A8	RSA digital signature verification	SHA2-256	SHS #4466
		TSF testing	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	Arm Cortex-A8	RSA digital signature verification	SHA2-256	SHS #4467
	Table 46 contains the complete list of cryptographic operations and CAVP certificates.						
	AA	*The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.*					

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>IPsec supports the conditioning of text-based pre-shared keys using SHA-1, SHA2-256, and SHA2-512 hash algorithms as specified in FIA_PSK_EXT.1. For more details on the pre-shared keys, see the TSS for FIA_PSK_EXT.1. IPsec supports SHA2-256 for KAS FFC and SHA2-256, SHA2-384, and SHA2-512 for KAS ECC as specified in FCS_CKM.1(a). For more details on KAS FFC and KAS ECC, see the TSS for FCS_CKM.1(a). IPsec supports SHA2-256, SHA2-384, and SHA2-512 for RSA signature generation and SHA-1, SHA2-256, SHA2-384, and SHA2-512 for RSA signature verification. For more details on the signature generation and verification algorithms, see the TSS for FCS_COP.1(b). IPsec also supports HMAC algorithms using SHA2-256, SHA2-384, and SHA2-512. For more details on the HMAC algorithms, see the TSS for FCS_IPSEC_EXT.1.

For trusted update, the RSA digital signature verification uses the SHA2-256 hash algorithm. For more details on digital signatures in trusted update, see the TSS for FPT_TUD_EXT.1.

For TSF testing (Whitelisting), the RSA digital signature verification uses the SHA2-256 hash algorithm. For more details on digital signatures in TSF testing, see the TSS for FPT_TST_EXT.1.</td></tr>
<tr><td>FCS_COP.1(g) (HMAC)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
IPsec supports the keyed-hash message authentication algorithms and key sizes specified in Table 41 using the HP FutureSmart QuickSec 5.1 meeting [FIPS180-4] (which supersedes FIPS 180-3 specified in the SFR) and [FIPS198-1]. IPsec uses truncated HMACs. Table 41 also shows the actual digest sizes and the IPsec truncated digest sizes. For more details on the required HMAC algorithms, see the TSS for FCS_IPSEC_EXT.1.

Table 41: HMAC algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Op env</th><th>Algorithm</th><th>Key size</th><th>Actual/Trunc. digest size</th><th>CAVP cert #</th></tr>
<tr><td rowspan="4">IPsec</td><td rowspan="4">HP FutureSmart QuickSec 5.1</td><td rowspan="4">Arm Cortex-A8</td><td>HMAC-SHA-1</td><td>160 bits</td><td>160/96 bits</td><td rowspan="4">HMAC #3711</td></tr>
<tr><td>HMAC-SHA2-256</td><td>256 bits</td><td>256/128 bits</td></tr>
<tr><td>HMAC-SHA2-384</td><td>384 bits</td><td>384/192 bits</td></tr>
<tr><td>HMAC-SHA2-512</td><td>512 bits</td><td>512/256 bits</td></tr>
</table>
Table 46 contains the complete list of cryptographic operations and CAVP certificates.
</td></tr>
<tr><td></td><td>AA</td><td>None</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FCS_IPSEC_EXT.1 (IPsec)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
The TOE uses IPsec to protect all communication channels required to satisfy O.COMMS_PROTECTION. IPsec must be enabled in the evaluated configuration. The management function for enabling IPsec is specified in the TSS for FMT_MOF.1.

IPsec supports both PSKs and X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange version 1 (IKEv1) protocol, and the following cryptographic algorithms to protect the channels.
• DH (dhEphem) P=2048, SHA2-256 (FCS_CKM.1(a))
• DSA (FCS_CKM.1(a))
  o L=2048, N=224
  o L=2048, N=256
  o L=3072, N=256
• ECDH (ephemeral unified) (FCS_CKM.1(a))
  o P-256, SHA2-256
  o P-384, SHA2-384
  o P-521, SHA2-512
• ECDSA P-256, P-384, and P-521 (FCS_CKM.1(a))
• RSA 2048-bit and 3072-bit signature generation/verification (FCS_COP.1(b))
• AES-CBC-128, AES-CBC-256, and AES-ECB-256 (FCS_COP.1(a))
• HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1(g))
• CTR_DRBG(AES) (FCS_RBG_EXT.1)
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale
	The TOE imports the RSA keys—in the form of X.509v3 certificates—used by IPsec in the evaluated configuration. It does not generate RSA keys. During the TOE's initial configuration, the administrator imports the TOE's RSA-based identity certificate and the matching RSA-based Certificate Authority (CA) root certificate from the Operational Environment as described in the [CCECG] section *Certificates*. The administrator also imports any other RSA-based CA certificates necessary to validate IPsec connections. For more information on the TOE's certificate management capabilities, see the TSS for FMT_MTD.1 for certificate importing. IPsec IKEv1 supports and allows either DH/DSA or ECDH/ECDSA in phase 1 to establish a protected connection using KAS FFC and KSA ECC, respectively. Random values generated for the KAS FFC or KSA ECC are generated by the TOE using the CTR_DRBG(AES) DRBG specified in FCS_RBG_EXT.1 and described in the TSS for FCS_RBG_EXT.1. The CTR_DRBG(AES) DRBG uses the AES-ECB-256 algorithm. For IKEv1, the TOE supports peer authentication using either RSA-based digital signatures (RSA 2048-bit and 3072-bit) or pre-shared keys. IKEv1 uses only Main Mode for Phase 1 exchanges to provide identity protection. (Aggressive Mode is not supported and is not a configurable option.) The encrypted IKEv1 payloads are required to use either AES-CBC-128 or AES-CBC-256. No other payload algorithms are allowed in the evaluated configuration. The TOE's IKEv1 supports the following DH Groups. The DH groups are specified using a defined group description as specified in [RFC3526] . • DH Group 14 (2048-bit MODP) • DH Group 15 (3072-bit MODP) • DH Group 16 (4096-bit MODP) • DH Group 17 (6144-bit MODP) • DH Group 18 (8192-bit MODP) All TOE cryptographic functions used by IPsec are implemented in the HP FutureSmart QuickSec 5.1 ([QuickSec51]) which is produced by INSIDE Secure. The TOE's Security Association (SA) lifetimes can be established based on the length of time, where the time values can be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs. The TOE's IPsec processes packets following the policy order defined in the Security Policy Database (SPD). The first matching policy is used to process the packet. The final policy in the SPD matches all unmatched packets and causes the TOE to discard the packet. The TOE's IPsec is conformant to the MUST/MUST NOT requirements of the following Internet Engineering Task Force (IETF) Request for Comments (RFCs). • [RFC3602] for use of AES-CBC-128 and AES-CBC-256 in IPsec

TOE SFRs	TOE SFR compliance rationale
	• [RFC4301] for IPsec • [RFC4303] for ESP • [RFC2407] and [RFC2408] for ISAKMP • [RFC2409] and [RFC4109] for IKEv1 • [RFC4868] for SHA-2 HMAC in IPsec The TOE does not support Extended Sequence Number (ESN). *IPsec/Firewall* The TOE's IPsec implementation contains a firewall. The firewall allows administrators to block and/or restrict access to TOE ports. Because [HCDPP] does not contain firewall requirements, the functionality of the firewall is not claimed in this ST, but its function is included in the packet processing description below. *Incoming packet processing* In a network context, the TOE is an endpoint versus being an intermediary such as a network switch. Thus, packets originate from and terminate at the TOE. When the TOE receives an incoming packet, it determines whether or not the packet is destined for the TOE. If not destined for the TOE, the packet is discarded. If destined for the TOE, the firewall rules are applied. The firewall rules map address templates to service templates. In essence, the rules map IP addresses to ports. The default rule is to discard (i.e., drop) all packets that do not match a firewall rule. This default rule can be modified by an administrator. Also, if the packet is not an IPsec protected packet, the packet is discarded except for the DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 service packets which are bypassed. The TOE's simplicity of the rule configuration helps to avoid overlapping rules, but if one or more overlapping rules exist, the first matching rule is the rule that is enforced. Administrators can add, delete, enable, and disable rules as well as modify the processing order of existing rules. If the packet is a request for a new connection, then the IKE negotiation is performed to establish SAs based on the connection rules in the SPD. This negotiation supports both pre-shared keys and certificates. Next, the packet is compared against the set of known Security Associations (SAs). If the packet fails to match an SA, the packet is discarded. The SA is checked to ensure that the SA's lifetime has not expired and that the amount of data allowed by the SA has not been exceeded. If any of these checks fail, the packet is discarded. If all the checks succeed, the IPsec portion of the packet processing is considered complete and the packet is processed as part of the connection's flow. *Outgoing packet processing* The TOE originates packets over established IPsec connections. Because of this, only protected (encrypted) packets are sent from the TOE to connected IT entities. The exceptions being for the DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 service packets which are bypassed. The TOE does not forward packets received from other devices.

TOE SFRs	TOE SFR compliance rationale	
	Protected packets being transmitted are compared to the SPD rules for that interface. Again, the first matching rule applies. Packets matching an SPD rule are encrypted and sent to the IT entity. All other packets are discarded. If this is the first transmission, an SA is created based on the SPD connection rules.	
	AA	*As per NIAP Technical Decision [*CCEVS-TD0157*] FCS_IPSEC_EXT.1.1: The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.* *As noted in section 4.4.1 of [*RFC4301*], the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.*
	Resp	The Summary section above provides a description of the packet processing.
	AA	*FCS_IPSEC_EXT.1.2: The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).*
	Resp	The VPN operates in transport mode only in the evaluated configuration.
	AA	*FCS_IPSEC_EXT.1.3: The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no "rules" are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.*
	Resp	Packets are processed following the order defined in the Security Policy Database (SPD). The first matching policy is used to process the packet. The final policy in the SPD matches all unmatched packets and causes the TOE to discard the packet.
	AA	*FCS_IPSEC_EXT.1.4: The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).*
	Resp	Algorithms: • AES-CBC-128 and AES-CBC-256 (FCS_COP.1(a)) • HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1(g))

TOE SFRs	TOE SFR compliance rationale	
	AA	*FCS_IPSEC_EXT.1.5: The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.*
	Resp	Only IKEv1 is supported in the evaluated configuration.
	AA	*FCS_IPSEC_EXT.1.6: The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.*
	Resp	Only AES-CBC-128 and AES-CBC-256 are used for encrypting the payload.
	AA	*FCS_IPSEC_EXT.1.7: The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.*
	Resp	Only Main Mode is used for Phase 1 exchanges. Aggressive Mode is not supported and is not a configurable option.
	AA	*FCS_IPSEC_EXT.1.9: The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.*
	Resp	The DH groups are specified using a defined group description as specified in [RFC3526].
	AA	*FCS_IPSEC_EXT.1.10: The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.*
	Resp	RSA-based digital signatures (RSA 2048-bit and 3072-bit) or pre-shared keys.
FCS_KYC_EXT.1 (Key chaining)		

Objective(s):	O.STORAGE_ENCRYPTION

Summary

The TOE uses a 256-bit drive-lock password (a.k.a. BEV) to unlock the TOE's field-replaceable SED. This BEV is stored as a key chain of one in a non-field replaceable nonvolatile storage (EEPROM) located inside the TOE. The TOE generates this BEV by making a single invocation request for 256-bits of data from the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 DRBG specified in FCS_RBG_EXT.1.

The BEV is automatically generated by the TOE when the TOE is first initialized and stored in non-field replaceable, nonvolatile memory. Afterwards, the BEV is never changed in the evaluated configuration; therefore, there are no claimed security management functions for the BEV in this ST. It is also never destroyed. No interfaces are provided to view the BEV or to retrieve the BEV; therefore, the BEV is never seen by a human (i.e., it is only known by the TOE).

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>AA</td><td>The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer [than] 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.</td></tr>
<tr><td></td><td>Resp</td><td>The drive-lock password (a.k.a. BEV) is a 256-bit binary value and generated using FCS_RBG_EXT.1.</td></tr>
<tr><td>FCS_RBG_EXT.1 (DRBG)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
<tr><td></td><td>O.STORAGE_ENCRYPTION</td></tr>
</table>
<u>Summary</u>
IPsec uses the CTR_DRBG(AES) DRBG algorithm from HP FutureSmart QuickSec 5.1 to generate key and key material. This DRBG supports the AES 256-bit algorithm. The AES-ECB-256 algorithm claimed in FCS_COP.1(a) for QuickSec 5.1 is used by this DRBG.

The SED drive-lock password generation mechanism uses the CTR_DRBG(AES) algorithm from the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 to generate the password (BEV). This DRBG supports the AES 256-bit algorithm. The AES-CTR-256 algorithm claimed in FCS_COP.1(a) for OpenSSL 2.0.4 is used by this DRBG.

Both DRBGs are seeded by a hardware-based entropy noise source. This entropy source provides 256 bits of minimum entropy.

Table 42: DRBG algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Op env</th><th>Modes & key sizes</th><th>CAVP cert #</th></tr>
<tr><td>IPsec</td><td>HP FutureSmart QuickSec 5.1</td><td>Arm Cortex-A8</td><td>CTR_DRBG(AES-256)</td><td>DRBG #2220</td></tr>
<tr><td>Drive-lock password (BEV)</td><td>HP FutureSmart OpenSSL FIPS Object Module 2.0.4</td><td>Arm Cortex-A8</td><td>CTR_DRBG(AES-256)</td><td>DRBG #2217</td></tr>
</table>
Table 46 contains the complete list of cryptographic operations and CAVP certificates.
</td></tr>
<tr><td></td><td>AA</td><td>For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>The TOE implements two DRBGs. One is used by IPsec and the other is used for the SED drive-lock password (BEV) generation.</td></tr>
<tr><td>FDP_ACC.1
(Subset access control)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr><tr><td></td><td>O.USER_AUTHORIZATION</td></tr></table><u>Summary</u> [HCDPP] predefines the subjects, objects, and operations. Table 21 and Table 22 of this ST list these values and enumerates the operations between the subjects and objects.</td></tr>
<tr><td></td><td>AA</td><td>It is covered by assurance activities for FDP_ACF.1.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FDP_ACF.1
(Security attribute based access control)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr><tr><td></td><td>O.USER_AUTHORIZATION</td></tr></table><u>Summary</u>
In this section, Table 21 is explained first followed by Table 22.

<u>Scan Create/Read/Modify/Delete D.USER.DOC in Table 21</u>

In order to scan a document, the user must be logged into the TOE via the Control Panel. When the job is scanned, the job is owned by the logged in user. Neither an administrator (U.ADMIN) nor another user (U.NORMAL) can create a scan job under a different user identity. The job owner can create, read, and delete a scan job, but cannot modify a scan job by design. The U.ADMIN can delete a scan job.

Required security attributes:

• Subject: Control Panel user identity/role

• Object: Job owner

<u>Scan Create/Read/Modify/Delete(Cancel) D.USER.JOB in Table 22</u></td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">In order to scan a document, the user must be logged into the TOE via the Control Panel. When the job is scanned (i.e., created), the job is owned by the logged in user. Neither U.ADMIN nor another user can create a scan job under a different user identity. The job owner can create, view scan status/log, and cancel a scan job owned by the job owner. An administrator (U.ADMIN) can view the scan status/log, and cancel a scan job. Neither the job owner or an administrator (U.ADMIN) can modify a scan job by design. Other U.NORMAL and unauthenticated users can view the scan status, but not the scan log.

Required security attributes:
• Subject: Control Panel user identity/role
• Object: Job owner</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 21 and Table 22.</td></tr>
<tr><td></td><td>Resp</td><td>See the description above.</td></tr>
<tr><td>FDP_DSK_EXT.1 (Disk data protection)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.STORAGE_ENCRYPTION</td></tr>
</table>
<u>Summary</u>
The TOE contains one field-replaceable, nonvolatile storage device. This device is a disk-based self-encrypting drive (SED).

[HCDPP] states that SEDs must be CC certified using the Full Disk Encryption (FDE) Encryption Engine (EE) collaborative PP (cPP). NIAP has issued Interim Guidance ([CCEVS-SED]) stating that until CC certified SEDs are readily available, FIPS 140-2 validated SEDs are sufficient for NIAP HCDPP evaluations. Table 43 lists the field-replaceable SED model used by all TOE models and its corresponding CMVP FIPS 140-2 certificate number.

Table 43: SED NIST CMVP certificate number
<table>
<tr><th>SED model</th><th>NIST CMVP cert #</th></tr>
<tr><td>Seagate model: ST500LT015 (500GB)
Hardware version: 1DJ142
Firmware version: 1002SED7</td><td>Cert #1826</td></tr>
</table>
The SED performs all of the storage encryption and decryption internally (i.e., the SED corresponds to the FDE EE) without any TOE or user intervention. The encryption and decryption implementation is built into the SED. The data is encrypted and stored by the SED as the SED receives the data. The SED decrypts the data when a read request is made. The standard Serial AT Attachment (SATA) interface is used to interface the TOE to the drive.
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">The TOE provides an SED drive-lock password (a.k.a. BEV) to the SED. The SED uses this password to decrypt the symmetric key it uses to encrypt and decrypt the data on the SED (i.e., the TOE corresponds the FDE AA). Only when the TOE provides the correct password to the SED can the SED's symmetric key be decrypted.

The TOE generates the initial drive-lock password when the TOE is initialized and stores it in the TOE's internal non-field replaceable nonvolatile memory (i.e., EEPROM). This password is never changed and is not accessible by any user.

SEDs typically have a small portion of space on the drive that is not encrypted. This unencrypted space is used by the drive to store its own key chains needed to encrypt and decrypt the rest of the storage. The SED uses the drive-lock password (BEV) provided by the TOE to encrypt and decrypt this key chain. The TOE has no control over this unencrypted space.

For more information on the SED drive-lock password, see the TSS for FCS_KYC_EXT.1.</td></tr>
<tr><td></td><td>AA</td><td>As per NIAP Technical Decision [CCEVS-TD0176]

If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The tester shall confirm that the specific SED is listed in the TSS, documented and verified to be CC certified against the FDE EE cPP.

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied.

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.</td></tr>
<tr><td></td><td>Resp</td><td>The Summary section above provides the necessary description for this assurance activity.</td></tr>
<tr><td>FDP_RIP.1(a)
(Document erase)</td><td colspan="2"><table><tr><th>Objective(s):</th><td>O.IMAGE_OVERWRITE</td></tr></table>
<u>Summary</u>
Note: The O.IMAGE_OVERWRITE objective limits the scope of this requirement to field-replaceable, nonvolatile storage devices.

User document data are stored on a field-replaceable, nonvolatile storage device, specifically a disk drive that is also an SED. These user document data are stored in the form of job files. When a job file is deleted (either automatically by the system or by request of a user), the TOE will overwrite the file.

The TOE calls this image overwrite feature "Managing Temporary Job Files." This feature contains three options of which only two are allowed to be used in the evaluated configuration. This restriction is documented in the [CCECG] section Managing temporary job files and must be enforced by the administrator.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">The administrator can select between either one of these two allowed options.

• Secure Fast Erase (overwrite 1 time)

• Secure Sanitize Erase (overwrite 3 times)

Secure Fast Erase overwrites a job file once using a static byte value of 0x48. Then the file is unlinked (deallocated) from the file system and the disk blocks comprising the file reassigned to free space in the file system.

Secure Sanitize Erase overwrites a job file three times. The first pass uses a static byte value of 0x48. The second pass uses a static byte value of 0xB7. The third pass uses pseudo-random values. Then, the file is unlinked (deallocated) from the file system and the disk blocks comprising the file reassigned to free space in the file system.

The third option is called "Non-Secure Fast Erase (no overwrite)." This option must not be selected in the evaluated configuration.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where image data is stored and how and when it is overwritten.</td></tr>
<tr><td></td><td>Resp</td><td>The TOE has a single field-replaceable, nonvolatile disk drive. User document data is in the form of job files on this drive. When a job file is deleted (either automatically by the system or by requested of a user), the TOE will overwrite the file.

The administrator can select between two options of file overwrite performed by the TOE. The Secure Fast Erase option performs a single pass overwrite using a static value. The Secure Sanitize Erase option performs a three pass overwrite where the first pass uses a static value, the second pass uses a different static value, and the third pass uses pseudo-random values. After the overwrite completes, the file is unlinked (deallocated) from the file system.</td></tr>
<tr><td>FIA_AFL.1 (Authentication failure handling)</td><td colspan="2"><table><tr><th>Objective(s):</th><td>O.USER_I&A</td></tr></table><u>Summary</u>
This SFR applies to the Local Device Sign In mechanism (used by the Control Panel, EWS, and RESTful interfaces). The only accounts associated with this mechanism is the Device Administrator account.

The lockout mechanism uses the following control values.

• Account lockout maximum attempts

• Account lockout interval

• Account reset lockout counter interval</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">The account lockout maximum attempts value allows an administrator to control the number of failed authentication attempts on an account before the account 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 rest lockout counter interval value; otherwise, the maximum attempts counter is reset to zero. When the maximum attempts count has been met, the account is locked for the amount of time specified by the account lockout interval value.

The account lockout interval value allows an administrator to control the length of time that the account remains locked. The administrator can choose a value between 60 seconds (1 minute) and 1800 seconds (30 minutes) inclusively in the evaluated configuration.

The account reset lockout counter interval value allows an administrator to specify the time (in seconds) in which the failed login attempts must occur before the account lockout maximum attempts counter is reset to zero. This value must be equal to or greater than the account lockout interval value.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of the actions in the case of authentication failure (types of authentication events, the number of unsuccessful authentication attempts, actions to be conducted), which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>When the administrator specified 3 to 10 authentication failures on an account are met, the account is locked for the period of time specified by the lockout interval. Caveats are:

• Consecutive failed authentication attempts using the same authentication credential count as a single failed authentication attempt.

• The failures must occur during the time value specified by the account reset lockout counter interval value; otherwise, the account lockout maximum attempts counter is reset to zero.</td></tr>
<tr><td>FIA_ATD.1
(User attribute definition)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.USER_AUTHORIZATION</td></tr></table><u>Summary</u>
<u>Control Panel users</u>

For Internal Authentication (i.e., the Local Device Sign In method), only one account exists in the evaluated configuration: Device Administrator. This account is a built-in account and is permanently assigned the Device Administrator PS which makes its role U.ADMIN. The user identifier is the Display name and the authenticator is a password. The Device Administrator Password's composition requirements are defined in FIA_PMG_EXT.1.

For each External Authentication method (i.e., LDAP Sign In and Windows Sign In), the user identifiers and passwords are stored on and verified by the External Authentication server. Also, the network group memberships are stored on the External Authentication server. Because these security attributes are not stored on and maintained by the TOE, they are not listed in FIA_ATD.1.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">User accounts from External Authentication methods are known as network user accounts. Each network user account can have zero or one PS (i.e., network user PS) associated with it that is used in calculating the user's session PS (i.e., the user's role). These PSs are stored on and maintained by the TOE. User session PS formulas are provided in FIA_USB.1 and described in the TSS for FIA_USB.1.

<u>EWS users</u>

The EWS authentication works very similarly to the Control Panel authentication.

For Internal Authentication (i.e., the Local Device Sign In method), only one account exists in the evaluated configuration: Device Administrator. This account is a built-in account and is permanently assigned the Device Administrator PS which makes its role U.ADMIN. It contains a user identifier known as the Display name and a password known as the Device Administrator Password. The Device Administrator Password's composition requirements are defined in FIA_PMG_EXT.1.

For each External Authentication method (i.e., LDAP Sign In and Windows Sign In), the user identifiers and passwords are stored on and verified by the External Authentication server. Also, the network group memberships are stored on the External Authentication server. Because these security attributes are not stored on and maintained by the TOE, they are not listed in FIA_ATD.1.

<u>RESTful users</u>

For the RESTful interface, this interface is an administrator-only interface used to manage the TOE over IPsec.

For Internal Authentication, the RESTful interface supports the Local Device Sign In method which requires the administrator to authenticate using the Device Administrator account. The Display name is used as the identifier and password is used as the authenticator. Both are maintained internally by the TOE. For External Authentication, the RESTful interface supports the Windows Sign In method which requires the user to be associated with the Device Administrator permission set.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of the user security attributes that the TOE uses to implement the SFR, which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>See the Summary section above.</td></tr>
<tr><td>FIA_PMG_EXT.1 (Password management)</td><td colspan="2"><table><tr><th>Objective(s):</th><td>O.USER_I&A</td></tr></table>
<u>Summary</u>
The TOE manages the following password.

• Device Administrator Password

The value of the Device Administrator Password is composed of any combination of upper and lower-case letters, numbers, and the special characters specified in FIA_PMG_EXT.1. Their length of the Device Administrator Password is configurable by the administrator and can be set to have a minimum of 15 or more characters. For more information on the TOE's password length management capabilities, see the TSS for FMT_MTD.1.

The Device Administrator Password is used by the Control Panel, EWS, and RESTful interfaces.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>AA</td><td>None</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FIA_PSK_EXT.1
(Pre-shared key composition)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
The TOE supports IPsec text-based, pre-shared keys and accepts bit-based, pre-shared keys.

The text-based keys can be from 22 characters to 128 characters in length and be composed of any combination of upper and lower case letters, numbers, and special characters that include the characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". The text-based keys are conditioned using the administrator selectable SHA-1, SHA2-256, or SHA2-512 hash algorithms specified in FCS_COP.1(c).

The TOE accepts bit-based pre-shared keys generated outside of the TOE. It does not generate bit-based keys except from the text-based keys mentioned above. It allows the administrator to enter a hexadecimal bit-based, pre-shared key. For information on this, see the TSS for FMT_MTD.1.
</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning.

If "bit-based pre-shared keys" is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.</td></tr>
<tr><td></td><td>Resp</td><td>Text-based keys are 22 to 128 characters in length, composed of the characters described in the Summary above, and are conditioned using SHA-1, SHA2-256, or SHA2-512.

Hexadecimal bit-based keys can be entered into the TOE as well.</td></tr>
<tr><td>FIA_UAU.1
(Timing of authentication)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.USER_I&A</td></tr>
</table>
<u>Summary</u>
<u>Control Panel</u>

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

• Viewing of Welcome message
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale

	• Resetting of Control Panel
	• Selection of Sign In
	• Selection of sign-in method from Sign In screen
	• Viewing of device status information
	• Changing display language for the session
	• Viewing of network connectivity status information
	• Viewing of help information
	• Viewing of system time
	
	The Control Panel user cannot perform any other TSF-mediated actions until after the user has been successfully authenticated.
	
	Users select the sign in method from a menu of sign in methods. The menu options vary depending on the number of External Authentication methods configured for the TOE. The Control Panel supports the following Internal and External Authentication methods in the evaluated configuration.
	• Internal Authentication method
	  o Local Device Sign In
	• External Authentication methods
	  o LDAP Sign In
	  o Windows Sign In (via Kerberos)
	
	The Local Device Sign In method is always available in the TOE. Local Device Sign In contains only one account—the built-in Device Administrator account—in the evaluated configuration. The username (display name) and password are maintained internally by the TOE. At the Control Panel, the user selects the Local Device Sign In method, selects Administrator Access Code (a.k.a. Device Administrator account) from a menu, and is then prompted for the Device Administrator Password.
	
	If an LDAP Sign In method is configured, that method will be one of the possible External Authentication methods displayed in the menu. This method allows for the use of an LDAP server, such as the Microsoft Active Directory server, for I&A. Both the username and password are maintained by the LDAP server. The TOE uses the LDAP version 3 protocol over IPsec to communicate to the LDAP server. If a user selects this method, the user must enter a valid LDAP account's username and password to be granted access to the TOE.

TOE SFRs	TOE SFR compliance rationale

If a Windows Sign In method is configured, that method will be one of the possible External Authentication methods displayed in the menu. This method allows for the use of a Windows domain server for I&A. Both the username and password are maintained by the Windows domain server. The TOE uses the Kerberos version 5 protocol over IPsec to communicate to the Windows domain server. If a user selects this method, the user must enter a valid Windows domain account's username and password to be granted access to the TOE.

Network interfaces

Most of the client network interfaces protected by IPsec perform authentication. Table 45 provides a list of the available IPsec client interfaces to the TOE, whether or not there's an authentication mechanism associated with the client interface, and a list of TSF-mediated actions prior to authentication, if any.

Table 44: IPsec client interfaces

IPsec client interface	Authentication?	TSF-mediated actions prior to authentication?
EWS	Yes	Select a sign in method
RESTful	Yes	No

EWS over IPsec

The EWS interface is a web browser-based administrative interface used to manage the TOE over IPsec. The EWS interface requires the user to sign in using the same sign in method menu options as provided by the Control Panel (i.e., Local Device Sign In, LDAP Sign In, and Windows Sign In when configured for these sign in methods). Table 45 shows any TSF-mediated actions prior to authentication for this protocol.

RESTful over IPsec

The RESTful interface is an administrative interface used to manage the TOE over IPsec.

The RESTful interface supports the Local Device Sign In method for I&A which requires the administrator to authenticate using the Device Administrator account. The Display name and password are maintained internally by the TOE. For External Authentication, the RESTful interface supports the Windows Sign In method which requires the user to be associated with the Device Administrator permission set. Table 45 shows any TSF-mediated actions prior to authentication for this protocol.

Other

Also see the TSS for FIA_UID.1.

AA	*The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).*

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>The Control Panel provides the Local Device Sign In method as the internal I&A mechanism and provides an LDAP Sign In method and Windows Sign In method as external I&A mechanisms.

Over the IPsec channel, EWS provides the same sign in methods as the Control Panel. The RESTful interface provides the Local Device Sign In and Windows Sign In methods.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces).</td></tr>
<tr><td></td><td>Resp</td><td>The Control Panel, EWS, and RESTful interfaces perform I&A.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers.</td></tr>
<tr><td></td><td>Resp</td><td><table><tr><th>External Authentication server</th><th>Protocol</th></tr><tr><td>LDAP server</td><td>LDAP version 3</td></tr><tr><td>Windows domain server</td><td>Kerberos version 5</td></tr></table></td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>On the Control Panel, the user can perform the following actions prior to I&A.
Viewing of Welcome message
Resetting of Control Panel
Selection of Sign In
Selection of sign-in method from Sign In screen
Viewing of device status information
Changing display language for the session
Viewing of network connectivity status information
Viewing of help information
Viewing of system time</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td></td><td>For EWS, the user can select a sign in method. For RESTful, there are no TSF-mediated actions prior to I&A.</td></tr>
<tr><td>FIA_UAU.7
(Protected authentication feedback)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.USER_I&A</td></tr></table><u>Summary</u>
The Control Panel (for Internal and External Authentication methods) and EWS (for Internal and External Authentication methods) display a dot for each password character typed by the user.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of the authentication information feedback provided to users while the authentication is in progress, which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>A dot is displayed for each password character typed by the user on the Control Panel and EWS for both Internal and External Authentication methods.</td></tr>
<tr><td>FIA_UID.1
(Timing of identification)</td><td colspan="2"><table><tr><td rowspan="2">Objective(s):</td><td>O.ADMIN_ROLES</td></tr><tr><td>O.USER_I&A</td></tr></table><u>Summary</u>
From the Control Panel, the user can perform the following actions prior to identification.
Viewing of Welcome message
Resetting of Control Panel
Selection of Sign In
Selection of sign-in method from Sign In screen
Viewing of device status information
Changing display language for the session
Viewing of network connectivity status information
Viewing of help information
Viewing of system time
Once the IPsec channel is successfully established, the following interfaces initiate their identification mechanisms. The following shows their TSF-mediated actions prior to identification.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>

EWS:
Select a sign in method
RESTful:
No TSF-mediated actions prior to identification

In all cases, the user cannot perform any other TSF-mediated actions than the ones listed above until after the user has been successfully identified.

For additional information on I&A, see the TSS for FIA_UAU.1.
<table>
<tr><td>AA</td><td>It is covered by the assurance activities for FIA_UAU.1.</td></tr>
<tr><td>Resp</td><td>n/a</td></tr>
</table>
</td></tr>
<tr><td>FIA_USB.1
(User-subject binding)</td><td>
<table>
<tr><th>Objective(s):</th><td>O.USER_I&A</td></tr>
</table>
<u>Summary</u>
<u>Control Panel User Identity Binding</u>

Once a Control Panel user has successfully signed in, a username and a role are bound to the subjects acting on behalf of that user.

For Internal Authentication, if the user signs in using the Local Device Sign In method, the bound username will be the Display name. Because the Device Administrator is the only Local Device Sign In account in the evaluated configuration, the username will be the Device Administrator account's Display name.

For External Authentication, if the user signs in using the LDAP Sign In method, the bound username will be the user's LDAP username. Similarly, if the user signs in using the Windows Sign In method, the bound username will be the user's Windows username.

<u>Control Panel and EWS User Role Binding</u>

The Control Panel user's role is determined by the user's session permission set (PS) that is bound to the subjects acting on behalf of that user. The Internal Authentication mechanism has one PS per user. The External Authentication mechanisms have one PS per authentication method, zero or one PS per user, and zero or one PS per network group to which the user belongs. For more information on permission sets, see the TSS for FMT_SMR.1.

The role associated with the Local Device Sign In method's Device Administrator account is always U.ADMIN. The TOE accomplishes this by setting the Device Administrator's session PS to the Device Administrator PS.

Device Administrator session PS = Device Administrator PS.

The role associated with an External Authentication method's user account (a.k.a. network user account) can be either U.ADMIN or U.NORMAL. The TOE accomplishes this using various combinations of permission sets (PSs) depending on the existence of certain types of PSs as described in the following paragraphs.
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale
	External user accounts introduce the concept of network groups. A network group (a.k.a. group) is a collection of zero or more external user accounts. Each External Authentication method defines and maintains its own groups. The members of a group are comprised of the external user accounts from that External Authentication method. An external user account can be associated with zero or more groups. A TOE administrator can associate zero or one PS to each group and zero or one PS to each external user account. These PS associations are stored and maintained on the TOE. A TOE administrator can create, modify, and delete these associations. By default, there are no PS associations for external user accounts and groups. For more information on the TOE's permission set association management, see the TSS for FMT_MSA.1. A PS is associated with each External Authentication method. These associations are also stored and maintained on the TOE. A TOE administrator can modify these associations. The TOE combines these various PSs using one of the following three methods. Method #1: If the external user account has a PS association, then the TOE combines the external user account's PS and the Device Guest PS to create the external user's session PS. User session PS = Network user PS + Device Guest PS. Method #2: If the external user account does not have an associated PS, the TOE obtains the groups to which the external user account is a member. For each of these groups, the TOE looks for matching group-to-PS associations. For each group-to-PS association match, the TOE combines that group's PS with any previously found group PSs. Once all matches have been found, the TOE combines these group PSs with the Device Guest PS to create the external user's session PS. User session PS = Network group PSs + Device Guest PS. Method #3: If there are no group-to-PS associations found for the external user account and the external user account does not have an associated PS, then the TOE combines the External Authentication method's PS and the Device Guest PS to create the external user's session PS. User session PS = External Authentication method PS + Device Guest PS. An administrator can associate one sign in method to a Control Panel application. This association limits the application to run only when the user signs in using the associated sign in method. For example, if an application is only associated with the LDAP Sign In method, a user must sign in using the LDAP Sign In method in order to run that application. The enforcement of this association is controlled by the "Allow users to choose alternate sign-in methods" function. If this function is enabled, then the sign in method permissions are ignored. If this function is disabled, then the user's session PS calculated above 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. *Remote User Identity Binding* Once an IPsec client computer has performed a successful IPsec connection with the TOE, the TOE uses the client's IP address as the client's user identifier for IPsec-related audit records. The EWS and RESTful interfaces support I&A mechanisms and use some form of username (e.g., Display name, Windows username) in audit records. In the case of EWS, the interface provides the same options as the Control Panel for sign in methods. Because of this, the Control Panel identity will be the Display name if the Local Device Sign In method is selected by the user, the LDAP username if the LDAP Sign In method is selected by the user, or the Windows username if the Windows Sign In method is selected by the user. From an auditing and access control perspective, the IP address is used by IPsec

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
when generating IPsec-related and network-related audit records. The EWS identity (i.e., Display name, LDAP username, Windows username) is used for all other identity-related purposes such as management-related tasks and audit records and access control enforcement and audit records.

In the case of the RESTful interface, both the Local Sign In method and Windows Sign In method are used for I&A. When authenticating via the Local Sign In Method, the RESTful identity will be the Display name. When authenticating via the Windows Sign In Method, the RESTful identity will be the Windows username.

From an auditing and access control perspective, the IP address is used by IPsec when generating IPsec-related and network-related audit records. The RESTful identity is used for all other identity-related purposes such as management-related tasks and audit records and access control enforcement and audit records.

<u>Remote User Role Binding</u>

In the case of EWS, the role is determined by the login account used by the user when logging in to the EWS interface.

In the case of RESTful interface, the role is determined by the login account used by the user when logging in to the RESTful interface.

<u>Other</u>

For all TOE I&A, once a user is signed in, the TOE does not provide the user with a way to modify their bound username and role.
<table>
<tr><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of rules for associating security attributes with the users who succeed identification and authentication, which is consistent with the definition of the SFR.</td></tr>
<tr><td>Resp</td><td>See the explanation in the Summary section above.</td></tr>
</table>
</td></tr>
<tr><td>FMT_MOF.1 (Management of functions)</td><td>
<table>
<tr><td>Objective(s):</td><td>O.ADMIN_ROLES</td></tr>
</table>
<u>Summary</u>
Allow users to choose alternate sign-in methods at the product control panel: With the "Allow users to choose alternate sign-in methods at the product control panel" function, the TOE provides an administrator the ability to enable and disable this function. When this function is disabled, it requires the user to sign in using the sign-in method associated with the selected application in order to access that application. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FIA_USB.1.

Control Panel full authentication: With the "Control Panel full authentication" function, the TOE provides an administrator the ability to enable and disable this function. This function must be enabled in the evaluated configuration. This function is restricted to U.ADMIN and can be performed through the EWS interface.

Windows Sign In: With the Windows Sign In function, the TOE provides an administrator the ability to enable and disable the Windows Sign In method. This function is restricted to U.ADMIN and can be performed through the EWS interface. At least one External Authentication mechanism must be enabled in the evaluated configuration. For related information, see the TSS for FIA_ATD.1 and TSS for FIA_UAU.1.

LDAP Sign In: With the LDAP Sign In function, the TOE provides an administrator the ability to enable and disable the LDAP Sign In method. This function is restricted to U.ADMIN and can be performed through the EWS interface.
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">At least one External Authentication mechanism must be enabled in the evaluated configuration. For related information, see the TSS for FIA_ATD.1 and TSS for FIA_UAU.1.

Account lockout: With the account lockout function, the TOE provides an administrator the ability to enable and disable the account lockout functions of the Device Administrator account. This function must be enabled in the evaluated configuration. This function is restricted to U.ADMIN. The Device Administrator's account lockout function can be enabled and disabled through the EWS interface. For related information, see the TSS for FIA_AFL.1.

Enhanced security event logging: With the enhanced security event logging function, the TOE provides an administrator the ability to enable and disable the generation of additional security events. This function must be enabled in the evaluated configuration. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FAU_GEN.1.

Managing Temporary Job Files: With this image overwrite function, the TOE provides an administrator the ability to determine which one of the three overwrite options is currently selected (i.e., determine the behavior of the overwrite function) and to modify the selection (i.e., modify the behavior of the overwrite function). In the evaluated configuration, an administrator must select between either Secure Fast Erase or Secure Sanitize Erase. The Non-Secure Fast Erase option must not be selected in the evaluated configuration. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FDP_RIP.1(a).

IPsec: With the IPsec function, the TOE provides an administrator the ability to enable and disable IPsec. IPsec must be enable in the evaluated configuration. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FCS_IPSEC_EXT.1.

Automatically synchronize with a Network Time Service: With the "Automatically synchronize with a Network Time Service" function, the TOE provides an administrator the ability to enable and disable NTS. NTS must be enabled in the evaluated configuration. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FPT_STM.1. Also see the management operations for "NTS server configuration data" in the TSS for FMT_MTD.1.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of the management functions that the TOE provides as well as user roles that are permitted to manage the functions, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.</td></tr>
<tr><td></td><td>Resp</td><td>The required information is provided in the Summary section above.</td></tr>
<tr><td>FMT_MSA.1
(Management of attributes)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr><tr><td></td><td>O.USER_AUTHORIZATION</td></tr></table><u>Summary</u>
The security attributes used by the TOE's access control mechanisms are described in FDP_ACF.1.

<u>Control Panel and EWS identities</u></td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale
	The TOE's access control mechanism uses the identities supplied by the Control Panel and EWS interfaces to control access to objects. This makes identities a subject security attribute of the access control mechanism. The TOE supports both Internal and External Authentication mechanisms in the evaluated configuration. ***Account identity (Internal Authentication mechanism):*** The TOE supports both Internal and External Authentication mechanisms. The Internal Authentication mechanisms contains only one account in the evaluated configuration. This account is the predefined Device Administrator account. This account has a Display name (i.e., subject identity). This account has the Device Administrator permission set permanently associated with it and is granted administrative access by default. The TOE does not provide any management operations for this account's identity. This is reflected in FMT_MSA.1 in Table 24. Because there are no management operations, the authorized roles entry is marked as not applicable (n/a) in Table 24. There is no default value property for the Display name because the account is predefined, thus, Table 24 shows this as not applicable (n/a). Similarly, no role can override the default value. ***Account identity (External Authentication mechanism):*** The External Authentication mechanisms are part of the Operational Environment. An external account's identity (a.k.a. user name or account name) is used as a subject security attribute to grant or deny access to access-controlled objects on the TOE. The external account identities are maintained by and on the External Authentication mechanisms. The TOE does not support any management operations on the account identities maintained by the External Authentication mechanisms as shown in FMT_MSA.1 in Table 24. Because the TOE has no control over these external account identities, there is no default value property (marked as n/a in Table 24) and no default value to override, thus, no role can override the default value. *Control Panel and EWS roles* The TOE's access control mechanism also uses permission sets to control access to objects on the TOE. Permission sets are used to determine user roles on the TOE. The TSS for FMT_SMR.1 contains an explanation of permission sets. Permission sets can be associated with internal user accounts, external user accounts (network users), network groups, and to External Authentication mechanisms. When a user logs in via the Control Panel or EWS, the user's session permission set is calculated by the TOE based on the rules described in the TSS for FIA_USB.1. The user's session permission set is used to determine a user's access to access-controlled objects on the TOE. ***Device Administrator permission set permissions:*** For the Device Administrator permission set permissions, the TOE provides the "view" management operation. This management operation is restricted to U.ADMIN. This permission set comes predefined in the TOE. Its default value property is considered permissive because its predefined value allows access to everything. Because this value is predefined, there is no default value override role associated with it. ***Device User and Device Guest permission set permissions:*** For the Device User permission set permissions and the Device Guest permission set permissions, the TOE provides the "modify and view" management operations. These management operations are restricted to U.ADMIN. These permission sets come predefined in the TOE. Their default value properties are considered restrictive because their predefined values are more restrictive than the Device Administrator permission set. Because these values are predefined, there is no default value override role associated with them.

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">Custom permission set permissions: For custom permission set permissions, the TOE provides the "create, modify, delete, and view" management operations. These management operations are restricted to U.ADMIN. A custom permission set's default value property is considered restrictive because its initial value upon creation is an empty permission set. This default value property cannot be overridden, therefore, there is no role that can override this default value.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FMT_MSA.3 (Initialization of attributes)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr>
<tr><td></td><td>O.USER_AUTHORIZATION</td></tr>
</table>
<u>Summary</u>
The descriptions have been provided in the TSS for FMT_MSA.1.
</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes which have properties of default values, which are defined in the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>The descriptions have been provided in the TSS for FMT_MSA.1.</td></tr>
<tr><td>FMT_MTD.1 (Management of TSF data)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr>
</table>
<u>Summary</u>
<u>TSF Data owned by U.NORMAL or associated with Documents or jobs owned by a U.NORMAL</u>

None: U.NORMAL doesn't own any TSF Data on the TOE.

<u>List of TSF Data not owned by U.NORMAL</u>

Device Administrator password: For the Device Administrator password, the TOE provides the "change" operation. The change operation allows an U.ADMIN to change the Device Administrator's password. This operation is restricted to U.ADMIN. For related information, see the TSS for FIA_PMG_EXT.1.

Permission set associations (except on the Device Administrator account): For all permission set associations for any external user account, network group, and External Authentication mechanism, the TOE provides the "add, delete, change, and view" management operations. These management operations are restricted to U.ADMIN. For related information, see the TSS for FDP_ACF.1 and TSS for FMT_MSA.1.

Permission set associations (only on the Device Administrator account): The Device Administrator account is the only internal, built-in account in the evaluated configuration. This account has the Device Administrator permission set permanently associated with it. The only management operation provided for the Device Administrator account's
</td></tr>
</table>

TOE SFRs	TOE SFR compliance rationale
	permission set association is the "view" operation. This can only be performed by a U.ADMIN (including the Device Administrator). For related information, see the TSS for FDP_ACF.1 and TSS for FMT_MSA.1. **Note:** Although audit records are TSF Data not owned by U.NORMAL, the TOE does not provide the ability to management audit records. *List of software, firmware, and related configuration data* ***IPsec CA and identity certificates:*** For the IPsec CA certificates, the TOE provides the "import and delete" operations through the EWS interface. The import operation adds a CA certificate to the TOE. The delete operation removes the selected CA certificate from the TOE. These operations are restricted to U.ADMIN. The TOE may contain one or more CA certificates. For the IPsec identity certificates, the TOE provides the "import and delete" operations for CA-signed identity certificates through the EWS interface. The import operation adds a CA-signed identity certificate to the TOE. The delete operation removes the CA-signed identity certificate from the TOE. These operations are restricted to U.ADMIN. The TOE initially comes with a self-signed identity certificate for IPsec. This self-signed identity certificate is generated during manufacturing of the TOE and cannot be deleted. This self-signed identity certificate must not be used in the evaluated configuration. Instead, the [CCECG] section *Certificates* instructs the U.ADMIN to import a CA-signed identity certificate and to set this CA-signed identity certificate as the TOE's network identity certificate. The TOE only allows one certificate to be its network identity certificate. ***IPsec pre-shared keys:*** For the IPsec pre-shared keys, the TOE provides the "set and change" operations. The set operation is used to set an initial pre-shared key value. The change operation allows an administrator to change the pre-shared key value. This operation is restricted to U.ADMIN. The hash algorithm used on the pre-shared key is selectable. The pre-shared keys are part of the IPsec policy. For related information on pre-shared keys, see the TSS for FIA_PSK_EXT.1. ***Internal clock settings:*** For the internal clock settings, the TOE provides the "change" operation. The change operation allows an administrator to change the date and time values (a.k.a. timestamp). This operation is restricted to U.ADMIN. For related information, see the TSS for FPT_STM.1. ***NTS server configuration data:*** For the NTS server settings, the TOE provides the "change" operation. The change operation allows an administrator to change the configuration data associated with the NTS server. This operation is restricted to U.ADMIN. For related information, see the TSS for FPT_STM.1. The NTS server function must be enabled for the NTS server configuration data to have an effect. For more information on the NTS server enablement, see the "Automatically synchronize with a Network Time Service" function in the TSS for FMT_MOF.1. ***Minimum password length:*** For the minimum password length settings, the TOE provides the "change" operation. The TOE provides minimum password length settings for the Device Administrator account. This operation is restricted to U.ADMIN. For related information, see the TSS for FIA_PMG_EXT.1. ***Account lockout maximum attempts:*** For the account lockout maximum attempts value, the TOE provides the "change" operation. This value allows an administrator to control the number of failed login attempts before the account 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 rest lockout counter interval value; otherwise, the maximum attempts counter is reset. The account lockout maximum attempt value affects the Device Administrator account. The change operation is restricted to U.ADMIN. For more information on account lockout in general, see the TSS for FIA_AFL.1. The account lockout function must be enabled for the account lockout maximum

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>attempts value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1.

Account lockout interval: For the account lockout interval value, the TOE provides the "change" operation. This value allows an administrator to control the length of time that the account remains locked. The administrator can choose a value between 60 and 1800 seconds inclusively in the evaluated configuration. The account lockout interval value affects the Device Administrator account. The change operation is restricted to U.ADMIN. For more information on account lockout in general, see the TSS for FIA_AFL.1. The account lockout function must be enabled for the account lockout interval value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1.

Account reset lockout counter interval: For the account reset lockout counter interval value, the TOE provides the "change" operation. This value allows an administrator to specify the time (in seconds) in which the failed login attempts must occur before the account lockout maximum attempts counter is reset. This value must be equal to or greater than the account lockout interval value. The account reset lockout counter interval value affects the Device Administrator account. The change operation is restricted to U.ADMIN. For more information on account lockout in general, see the TSS for FIA_AFL.1. The account lockout function must be enabled for the account reset lockout counter interval value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1.

Session inactivity timeout: For the session inactivity timeout, the TOE provides the "change" operation. The change operation allows an administrator to change the amount of time of inactivity before automatically logging out the user from an interactive session. This timeout works for both Control Panel and EWS sessions. The Control Panel and EWS interfaces have independent session inactivity timeout values. The change operation is restricted to U.ADMIN for both interfaces. For related information, see the TSS for FTA_SSL.3.
<table>
<tr><td>AA</td><td>None</td></tr>
<tr><td>Resp</td><td>n/a</td></tr>
</table>
</td></tr>
<tr><td>FMT_SMF.1 (Management functions)</td><td>
<table>
<tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr>
<tr><td></td><td>O.ADMIN_ROLES</td></tr>
<tr><td></td><td>O.USER_AUTHORIZATION</td></tr>
</table>
<u>Summary</u>
Table 26 in FMT_SMF.1 provides a mapping of each management function to its respective management SFR, to its objectives, and to the respective management SFR's TSS page. The SFR's TSS provides a more detailed description of the matching management function.

The following objectives do not have security management functionality defined for them in this ST.

• O.KEY_MATERIAL
• O.STORAGE_ENCRYPTION
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">O.TSF_SELF_TEST
O.UPDATE_VERIFICATION</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FMT_SMR.1
(Security roles)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.ACCESS_CONTROL</td></tr>
<tr><td></td><td>O.ADMIN_ROLES</td></tr>
<tr><td></td><td>O.USER_AUTHORIZATION</td></tr>
</table>
<u>Summary</u>
The TOE supports two roles:
U.ADMIN
U.NORMAL
The TOE can associate users with roles. The Device Administrator account (available through the Control Panel, EWS, and RESTful interfaces) is U.ADMIN.
<u>Permission sets</u>
The TOE implements roles through the use of permission sets. Permission sets are used to determine which Control Panel applications a Control Panel user can access and which EWS interfaces an EWS user can access. A permission set contains a list of allowed permissions where each permission determines access to a single Control Panel application or a single EWS interface.
The TOE contains the following built-in permission sets.
Device Administrator—Grants administrative capabilities
Device User—Grants typical user capabilities
Device Guest—Grants capabilities to non-signed in users
These built-in permission sets cannot be renamed or deleted. The Device Administrator permission set cannot be modified, but an administrator can modify the permissions in the Device User and Device Guest permission sets. In the evaluated configuration, the Device Guest permission set is empty (i.e., contains no permissions) by default. (Device Guest is mentioned here because its definition is used in the TSS for FIA_USB.1.)
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">As an alternative to built-in permission sets, administrators can create custom permission sets that allow an administrator to better map the TOE's permissions to the usage model of their organization. Administrators can also modify and delete any existing custom permission sets. By default, the TOE comes with no custom permission sets.

Besides user accounts, permission sets can also be assigned to sign in methods—Local Device Sign In, LDAP Sign In, and Windows Sign In—and network groups to which an external user account is a member. (A network group is a collection of external user accounts located on a single External Authentication mechanism. The network group and group members are defined on the External Authentication mechanism.)

When a user logs in to the TOE, their session permission set is determined by a combination of factors. For more details on how permission sets are determined, see the TSS for FIA_USB.1.

All permission sets are stored and maintained locally on the TOE. This means that the permission sets for the internal user accounts, external user accounts, authentication mechanisms, and network groups are all stored and maintained locally on the TOE.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FPT_KYP_EXT.1 (Key chain key protection)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.KEY_MATERIAL</td></tr></table><u>Summary</u>
As per FCS_KYC_EXT.1, the key chain is a key chain of one containing only the BEV. The BEV is stored in non-field replaceable, nonvolatile storage (EEPROM) located inside the TOE. For more information on the key chain and BEV, see the TSS for FCS_KYC_EXT.1.</td></tr>
<tr><td></td><td>AA</td><td>None</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td>FPT_SKP_EXT.1
(Key viewing protection)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
The TOE is a closed system and does not provide an interface to read pre-shared keys, symmetric keys, or private keys. As a closed system, it does not allow administrators to read memory or to access storage directly.

The TOE's EWS provides an interface to enter IPsec pre-shared key values. This interface does not allow the administrator to query the current pre-shared key value. No other external interfaces allow for the entering or reading of pre-shared keys.

The TOE stores the IPsec pre-shared keys in a file on the field-replaceable SED. This file is not accessible through any interface. For more details on the IPsec pre-shared keys, see the TSS for FCS_CKM.4, TSS for FCS_IPSEC_EXT.1, and TSS for FIA_PSK_EXT.1.

The SED drive-lock password (a.k.a. BEV) can be considered a symmetric key. This password is stored in cleartext in EEPROM, but the TOE does not provide an interface to view this key or to access the EEPROM. For more details on the SED drive-lock password, see the TSS for FCS_KYC_EXT.1.

Ephemeral asymmetric and symmetric keys created and used in IPsec sessions are inaccessible by any user because the TOE does not provide a user interface to read memory.

The TOE's private asymmetric keys found in X.509v3 certificates (used by IPsec) can be imported by the TOE, but the EWS interface does not display the private keys contained in these certificates.
</td></tr>
<tr><td>AA</td><td>The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.</td></tr>
<tr><td>Resp</td><td>The TOE is a closed system and does not provide an interface to read pre-shared keys, symmetric keys, or private keys. The description above provides extended details.</td></tr>
<tr><td>FPT_STM.1
(Time stamps)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.AUDIT</td></tr>
</table>
<u>Summary</u>
Note: Although [HCDPP] only maps O.AUDIT to FPT_STM.1, it is worth noting that reliable timestamps are also used by O.COMMS_PROTECTION and O.UPDATE_VERIFICATION when validating the validity period of certificates and by O.USER_I&A when performing session inactivity timeouts and authentication failure handling.

The TOE contains an internal system clock that is used to generate reliable timestamps. The TOE requires the use of an NTS service to keep the internal system clock's time synchronized. Only administrators can manage the system clock and the TOE's configuration of NTS.
</td></tr>
<tr><td>AA</td><td>The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>Resp</td><td>The TOE contains an internal system clock that is synchronized using an NTS.</td></tr>
<tr><td>FPT_TST_EXT.1
(TSF testing)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.TSF_SELF_TEST</td></tr>
</table>
<u>Summary</u>
The TOE contains TSF testing functionality called Whitelisting to help ensure only authentic, known-good System firmware files that have not been tampered with are loaded into memory.

During the load process, Whitelisting validates the integrity of system firmware files using RSA-2048 with SHA2-256. If the integrity check of a system firmware file fails, Whitelisting will reboot the HCD and the Basic Input/Output System (BIOS) will hold on boot with an error message displayed on the Control Panel UI.

The TOE Whitelists and checks dynamic-link libraries (DLLs) and executables that have been signed with Microsoft Authenticode signatures. This includes kernel files, device drivers, and applications.

Whitelisting uses the HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation for both the RSA 2048-bit and SHA2-256 algorithms. For additional details on these algorithms, see the TSS for FCS_COP.1(b) and TSS for FCS_COP.1(c).
</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.</td></tr>
<tr><td></td><td>Resp</td><td>The TOE performs Whitelisting of firmware files while booting. If any of the files fail the integrity check, the TOE reboots and the BIOS will hold on boot with an error message displayed on the Control Panel UI. More detail is provided above.</td></tr>
<tr><td>FPT_TUD_EXT.1
(Trusted update)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.UPDATE_VERIFICATION</td></tr>
</table>
<u>Summary</u>
The TOE's firmware can be updated by an administrator by downloading an update image from the HP Inc. Software Depot kiosk (website) and installing it on the TOE.

Kiosk: https://h30670.www3.hp.com/portal/swdepot/kioskLogin.do

Each update image is digitally signed by HP using the RSA 2048-bit and SHA2-256 algorithms. Each HCD has a factory-installed public key certificate from HP used by the TOE for verifying the update image's digital signature.

Once the update image is downloaded from the kiosk and loaded onto the Administrative Computer, the update image can be uploaded to the TOE through the TOE's EWS interface. Once uploaded, the TOE performs digital signature verification on each update image prior to installing using the RSA 2048-bit and SHA2-256 algorithms and the factory installed certificate. If the TOE's signature verification fails, the TOE won't allow the update to proceed. The TOE
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">uses the HP FutureSmart Rebex Total Pack 2017 R1 implementation of these algorithms. The RSA 2048-bit algorithm is defined in FCS_COP.1(b). The SHA2-256 hash algorithm is defined in FCS_COP.1(c). The [CCECG] section Updating TOE firmware describes the steps to update the TOE.

The current version of both the System firmware and the Jetdirect Inside firmware can be obtained through the following interfaces. How to obtain the firmware versions using these interfaces is described in the [CCECG] section Verify firmware versions.

• Control Panel

• EWS

Note: The HP Inc. Software Depot kiosk provides a SHA2-256 published hash of the update image and a Windows OS utility program that can be downloaded and used to verify the hash. Once downloaded, the update image can be verified on a separate computer prior to installation on the TOE using the published hash and the Windows OS utility program. Because the published hash verification is not performed by the TSF, the SHA2-256 published hash verification method is excluded from this SFR.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.</td></tr>
<tr><td></td><td>Resp</td><td>The TOE uses a digital signature to verify update images. The signature uses RSA 2048-bit and SHA2-256. The public key certificate used to validate the signatures is factory-installed on the TOE.

The TOE's update images can be downloaded from the HP Inc. Software Depot kiosk and installed using the TOE's EWS interface in the evaluated configuration.

The current version of both the System firmware and the Jetdirect Inside firmware can be obtained through the following interfaces.

• Control Panel

• EWS</td></tr>
<tr><td>FTA_SSL.3 (Interactive session termination)</td><td colspan="2"><table><tr><td>Objective(s):</td><td>O.USER_I&A</td></tr></table><u>Summary</u>
This SFR applies to the interactive sessions for the Control Panel and EWS. The TOE's RESTful interface does not support the concept of sessions.

<u>Control Panel</u>

The TOE supports an inactivity timeout for Control Panel sessions. If a signed in user is inactive for longer than the specified period, the user is automatically signed off of the TOE. The inactivity period is configurable by the administrator via the EWS (HTTP) and Control Panel interfaces. A single Control Panel inactivity period setting</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>exists per TOE. This setting is separate from the EWS setting. For more information on configuring the Control Panel's session timeout, see the TSS for FMT_MTD.1.

<u>EWS</u>

The TOE supports an inactivity timeout for EWS interactive sessions. The EWS session timeout setting is used to set the inactivity timeout period. This setting is configurable via the EWS interface. This setting is separate from the Control Panel setting. For more information on configuring the EWS's session timeout, see the TSS for FMT_MTD.1.
<table>
<tr><td>AA</td><td>The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.</td></tr>
<tr><td>Resp</td><td>All Control Panel and EWS sessions support session termination. Both have administratively configurable timeout periods.</td></tr>
</table>
</td></tr>
<tr><td>FTP_ITC.1
(Trusted channel)</td><td>
<table>
<tr><td>Objective(s):</td><td>O.AUDIT</td></tr>
<tr><td></td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
The TOE uses IPsec to provide a trusted communications channel between itself and all authorized IT entities. Each channel is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

The TOE provides and initiates trusted communication channels to the following authorized IT entities.
• authentication server
• DNS server
• FTP server
• NTS server
• SharePoint server
• SMB server
• SMTP server
• syslog server (audit server)
• WINS server
For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1.
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.</td></tr>
<tr><td></td><td>Resp</td><td>All trusted communications channels to authorized IT entities use IPsec.</td></tr>
<tr><td>FTP_TRP.1(a) (Administrator trusted path)</td><td colspan="2">
<table>
<tr><td>Objective(s):</td><td>O.COMMS_PROTECTION</td></tr>
</table>
<u>Summary</u>
The TOE uses IPsec to provide a trusted communication path between itself and remote administrators. Each path is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.
The following interfaces are the remote administrative interfaces of the TOE in the evaluated configuration.
• EWS (via a web browser)
• RESTful
For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1.
</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.</td></tr>
<tr><td></td><td>Resp</td><td>All remote administrative interfaces use IPsec. The remote administrative interfaces are EWS and RESTful.</td></tr>
</table>

7.1.2 CAVP certificates

Table 46 contains a complete list of cryptographic operations and their CAVP certificates claimed by this ST. It also includes the information required to satisfy [CCEVS-PL05].

The CAVP operational environment is the same for all cryptographic implementations.

- Arm Cortex-A8

Table 45: CAVP certificates

Usage	Implementation	SFR	Standard and operation	CAVP certificate
IPsec with IKEv1	HP FutureSmart QuickSec 5.1	FCS_CKM.1(a) (TSS page 95)	*[NIST SP 800-56A]* KAS FFC DH (dhEphem) KARoles: Initiator, Responder FB: SHA: SHA2-256 FC: SHA: SHA2-256 Prerequisite: SHS #4474, DSA #1432, DRBG #2220	CVL #1999
			[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

Usage	Implementation	SFR	Standard and operation	CAVP certificate
			[NIST SP 800-56A] KAS ECC Ephemeral Unified: KARoles: Initiator, Responder EC: Curve: P-256 SHA: SHA2-256 ED: Curve: P-384 SHA: SHA2-384 EE: Curve: P-521 SHA: SHA2-512 Prerequisite: SHS #4474, ECDSA #1501, DRBG #2220	CVL #1999
			[FIPS PUB 186-4] KAS ECC ECDSA Key Pair Gen: Curves: P-256, P-384, P-521 Prerequisite: SHS #4474, DRBG #2220	ECDSA #1501

Usage	Implementation	SFR	Standard and operation	CAVP certificate
		FCS_COP.1(a) (TSS page 102)	*[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

Usage	Implementation	SFR	Standard and operation	CAVP certificate
		FCS_COP.1(b) (TSS page 103)	*[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, 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	RSA #2996
		FCS_COP.1(c) (TSS page 104)	*[FIPS 180-3 and 180-4]* SHA-1, SHA2-256, SHA2-384, SHA2-512	SHS #4474

Usage	Implementation	SFR	Standard and operation	CAVP certificate
		FCS_COP.1(g) (TSS page 107)	*[FIPS 198-1]* HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Prerequisite: SHS #4474	HMAC #3711
		FCS_RBG_EXT.1 (TSS page 113)	*[NIST SP 800-90A Rev. 1]* CTR_DRBG(AES) Counter Modes: AES-256 (Uses AES-ECB-256) Prerequisite: AES #5567	DRBG #2220
Drive-lock password (BEV) generation	HP FutureSmart OpenSSL FIPS Object Module 2.0.4	FCS_COP.1(a) (TSS page 102)	*[FIPS PUB 197 (AES) and NIST SP 800-38A (CTR)]* AES-CTR Modes: Encrypt Key lens: 256 (bits) AES-ECB Modes: Encrypt Key lens: 256 (bits)	AES #5563

Usage	Implementation	SFR	Standard and operation	CAVP certificate
		FCS_RBG_EXT.1 (TSS page 113)	*[NIST SP 800-90A Rev. 1]* CTR_DRBG(AES) Counter Modes: AES-256 (Uses AES-CTR-256) Prerequisite: AES #5563	DRBG #2217
Trusted update (RSA sig(ver))	HP FutureSmart Rebex Total Pack 2017 R1	FCS_COP.1(b) (TSS page 103)	*[FIPS PUB 186-4]* RSA 186-4 *Signature verification PKCS1.5* Mod 2048 SHA: SHA2-256 Prerequisite: SHS #4466	RSA #2993
		FCS_COP.1(c) (TSS page 104)	*[FIPS 180-3 and 180-4]* SHA2-256	SHS #4466
TSF testing (Whitelisting) (RSA sig(ver))	HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937	FCS_COP.1(b) (TSS page 103)	*[FIPS PUB 186-4]* RSA 186-4 *Signature verification PKCS1.5* Mod 2048 SHA: SHA2-256 Prerequisite: SHS #4467	RSA #2994
		FCS_COP.1(c) (TSS page 104)	*[FIPS 180-3 and 180-4]* SHA2-256	SHS #4467

8 Abbreviations, Terminology and References

8.1 Abbreviations

AA

Assurance Activity

AES

Advanced Encryption Standard

AH

Authentication Header (IPsec)

Arm

Advanced RISC Machine

ASCII

American Standard Code for Information Interchange

BEV

Border Encryption Value

CA

Certificate Authority

CAVP

Cryptographic Algorithm Validation Program

CBC

Cipher Block Chaining

CC

Common Criteria

CCEVS

Common Criteria Evaluation and Validation Scheme

CCITT

Consultative Committee for International Telephony and Telegraphy

cert

certificate

cPP

Collaborative Protection Profile

CSEC

The Swedish Certification Body for IT Security

CSP

Critical Security Parameter

CTR

Counter mode

CTR_DRBG

Counter mode DRBG

CVL

Component Validation List

DEK

Data Encryption Key

DH

Diffie-Hellman

DLL

Dynamic-Link Library

DNS

Domain Name System

DRBG

Deterministic Random Bit Generator

DSA

Digital Signature Algorithm

DSS

Digital Sending Software

EAL

Evaluated Assurance Level

ECB

Electronic Code Book

ECC

Elliptic Curve Cryptography

ECDH

Elliptic Curve Diffie-Hellman

ECDSA

Elliptic Curve Digital Signature Algorithm

EE

Encryption Engine (FDE)

EEPROM

Electrically Erasable Programmable Read-Only Memory

EIA

Electronic Industries Alliance

ESN

Extended Sequence Numbers (IPsec)

ESP

Encapsulating Security Payload (IPsec)

EWS

Embedded Web Server

FDE

Full Drive Encryption

FFC

Finite Field Cryptography

FIPS

Federal Information Processing Standard

HCD

Hardcopy Device

HCDPP

Hardcopy Device Protection Profile

HMAC

Hashed Message Authentication Code

HP

Hewlett-Packard

I&A

Identification and Authentication

IETF

Internet Engineering Task Force

IKE

Internet Key Exchange (IPsec)

IP

Internet Protocol

IPv4

IP version 4

IPv6

IP version 6

IPsec

Internet Protocol Security

ISAKMP

Internet Security Association Key Management Protocol (IPsec)

ITU-T

International Telegraph Union Telecommunication Standardization Sector

KAS

Key Agreement Scheme

kbps

Kilobits Per Second

KDF

Key Derivation Function

LAN

Local Area Network

LDAP

Lightweight Directory Access Protocol

MFP

Multifunction Printer

MODP

Modular Exponential

n/a

Not applicable

NFC

Near Field Communication

NIAP

National Information Assurance Partnership

NIST

National Institute of Standards and Technology

NTLM

Microsoft NT LAN Manager

NTS

Network Time Service

OSP

Organizational Security Policy

OXP

Open Extensibility Platform

OXPd

OXP device layer

PDF

Portable Document Format

PKCS

Public-Key Cryptography Standards

PP

Protection Profile

PS

Permission Set

PSK

Pre-Shared Key

REST

Representational State Transfer (a.k.a. RESTful)

RESTful

See REST

RFC

Request for Comments

RSA

Rivest-Shamir-Adleman

SA

Security Association

SAR

Security Assurance Requirement

SATA

Serial AT Attachment

SED

Self-Encrypting Drive

SFR

Security Functional Requirement

SHA

Secure Hash Algorithm

SHS

Secure Hash Standard

SMB

Server Message Block

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SP

Special Publication

SPD

Security Policy Database (IPsec)

SPD

Security Problem Definition (CC)

SSC

Security Subsystem Class

SSH

Secure Shell

ST

Security Target

TCG

Trusted Computing Group

TIA

Telecommunications Industry Association

TLS

Transport Layer Security

TOE

Target of Evaluation

TSF

TOE Security Functionality

TSP

TOE Security Policy

TSS

TOE Summary Specification

UI

User Interface

USB

Universal Serial Bus

W3C

World Wide Web Consortium

WINS

Windows Internet Name Service

WLAN

Wireless Local Area Network

WS

Web Services

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 (both administrator and user) and/or password for each user of the product.

Border Encryption Value (BEV)

A secret value passed to a storage encryption component such as a self-encrypting storage device.

Control Panel Application

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

Data Encryption Key (DEK)

A key used to encrypt data-at-rest.

Device Administrator Password

The password used to restrict access to administrative tasks via EWS, RESTful, and the Control Panel interfaces. 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 ST.

Intermediate Key

A key used in a point between the initial user authorization and the DEK.

Near Field Communication (NFC)

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

Submask

A submask is a bit string that can be generated and stored in a number of ways, such as passphrases, tokens, etc.

TOE Owner

A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

User Security Attributes

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

8.3 References

CC **Common Criteria for Information Technology Security Evaluation**

Version 3.1R5

Date April 2017

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

CCECG **Preparatory Procedures and Operational Guidance for the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner**

Author(s) HP Inc.

Date TBD

CCEVS-PL05 **Applicability and Relationship of NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS)**

Date 2014-11-04

Location https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-5-update1.pdf

CCEVS-SED **Interim Guidance for Evaluation of Self-Encrypting Drives for the Hard Copy Device Protection Profile**

Author(s) NIAP

Date 2015-11-06

Location https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/HCD%20Evaluation%20of%20SEDs%20v2.pdf

CCEVS-TD0074 **FCS_CKM.1(a) Requirement in HCD PP v1.0**

Date 2015-12-15

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=77

CCEVS-TD0157 **FCS_IPSEC_EXT.1.1 - Testing SPDs**

Date 2017-06-15

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=161

CCEVS-TD0176 **FDP_DSK_EXT.1.2 - SED Testing**

Date 2017-04-11

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=180

CCEVS-TD0219 **NIAP Endorsement of Errata for HCD PP v1.0**

Date 2017-07-07

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=224

Assurance Activities for Key Transport

CCEVS-TD0253	Date	2017-11-08
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=259
CCEVS-TD0261	**Destruction of CSPs in flash**	
	Date	2017-11-14
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=267
CCEVS-TD0299	**Update to FCS_CKM.4 Assurance Activities**	
	Date	2018-03-16
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=305
CCEVS-TD0393	**Require FTP_TRP.1(b) only for printing**	
	Date	2019-02-26
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=403
FIPS180-4	**Secure Hash Standard (SHS)**	
	Date	2015-08-04
	Location	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-4	**Digital Signature Standard (DSS)**	
	Date	2013-07-19
	Location	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS197	**Advanced Encryption Standard (AES)**	
	Date	2001-11-26
	Location	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
FIPS198-1	**The Keyed-Hash Message Authentication Code (HMAC)**	
	Date	2008-07-16
	Location	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

HCDPP	**Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community**	
	Version	1.0
	Date	2015-09-10
	Location	https://www.niap-ccevs.org/pp/pp_hcd_v1.0.pdf
HCDPP-ERRATA	**Protection Profile for Hardcopy Devices - v1.0, Errata #1, June 2017**	
	Version	1.0
	Date	2017-06
	Location	https://www.niap-ccevs.org/pp/pp_hcd_v1.0-err.pdf
ISO-10118-3	**Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions**	
	Version	ISO/IEC 10118-3:2004
	Date	2004-03
	Location	https://www.iso.org/standard/39876.html
KMD	**Key Management Description for HP Inc. HCDs**	
	Author(s)	HP Inc.
	Date	September 2018
8500_N9120-UG	**HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide**	
	Author(s)	HP Inc.
	Date	9/2018
8500_N9120-IG	**HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide**	
	Author(s)	HP Inc.
	Date	10/2017
QuickSec51	**QuickSec 5.1 Toolkit Reference Manual**	

Author(s) INSIDE Secure

Version 1.0

Date December 2009

RFC2407 **The Internet IP Security Domain of Interpretation for ISAKMP**

Author(s) D. Piper

Date 1998-11-01

Location http://www.ietf.org/rfc/rfc2407.txt

RFC2408 **Internet Security Association and Key Management Protocol (ISAKMP)**

Author(s) D. Maughan, M. Schertler, M. Schneider, J. Turner

Date 1998-11-01

Location http://www.ietf.org/rfc/rfc2408.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

RFC3526 **More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)**

Author(s) Tero Kivinen, Mika Kojo

Date May 2003

Location https://www.ietf.org/rfc/rfc3526.txt

RFC3602 **The AES-CBC Cipher Algorithm and Its Use with IPsec**

Author(s) S. Frankel, R. Glenn, S. Kelly

Date 2003-09-01

Location http://www.ietf.org/rfc/rfc3602.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

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

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**

Date 2001-12-01

Location https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

SP800-56A-Rev3 **Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography**

Date 2018-04-16

Location https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf