# HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, HP Color LaserJet Managed MFP E47528

## Security Target

| | |
|---|---|
| **Version:** | **1.0** |
| **Status:** | **Final** |
| **Last Update:** | **2023-07-21** |
| **Classification:** | **Public** |

# Trademarks

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

- HP®
- LaserJet®

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

- Arm®
- Cortex®

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

- Kerberos™

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

- Microsoft®
- SharePoint®
- Windows®

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

- INSIDE Secure®
- QuickSec®

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

- OpenSSL®

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

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

# Revision History

| Version | Date | Author(s) | Description |
|---|---|---|---|
| 1.0 | 2023-07-21 | HP Inc. | Public version for evaluation. |

# Table of Contents

# List of Tables

# 1 Introduction

## 1.1 Security Target Identification

| | |
|---|---|
| Title: | **HP LaserJet Enterprise MFP M430/M431,**<br>**HP Color LaserJet Enterprise MFP M480,**<br>**HP LaserJet Managed MFP E42540,**<br>**HP Color LaserJet Managed MFP E47528**<br><br>**Security Target** |
| Version: | 1.0 |
| Status: | Final |
| Date: | 2023-07-21 |
| Author: | HP Inc. |
| Certification Body: | OCSI |
| Certification ID: | OCSI/CERT/ATS/18/2022 |
| Keywords: | Common Criteria, HCD, HCDPP, Hardcopy Device, MFP, LaserJet Managed, M430, M431, M480, E42540, E47528 |

## 1.2 TOE Identification

The TOE is the HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, and HP Color LaserJet Managed MFP E47528 multifunction printers (MFPs) with HP FutureSmart 5.3.2 Firmware. The complete list of models and firmware versions is provided in Table 1.

## 1.3 TOE Type

The TOE type is a hardcopy device (HCD) also known as a multifunction printer (MFP).

## 1.4 TOE Overview

This document is the Common Criteria (CC) Security Target (ST) for the HP 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.

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

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
- Public Switched Telephone Network (PSTN) fax-network separation (if PSTN fax function is present)

### 1.4.1 Required and Optional Hardware, Software, and Firmware

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.

- Client computers network connected to the TOE in a non-administrative computer role
- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- Microsoft SharePoint®
- The following remote file systems:
    - File Transfer Protocol (FTP)

    - Server Message Block (SMB)
- A Simple Mail Transfer Protocol (SMTP) gateway
- Telephone line connection

### 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 printing, copying, faxing, scanning, and storing/retrieving documents. The physical environment should be reasonably controlled and/or monitored where physical tampering of the HCDs would be evident and noticed.

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

The 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
    - Printing, scanning, copying
    - Configuration
    - Auditing
    - Verifying software updates
    - Verifying HCD function
- Conditionally mandatory use cases
    - Sending PSTN faxes
    - Receiving PSTN faxes
    - Storing and retrieving documents
    - Field-replaceable nonvolatile storage devices

## 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.

All TOE models use the same Jetdirect Inside firmware version.

- JOL25030046

The TOE includes the following System firmware versions.

- 2503252_000044 (HP FutureSmart 5.3.2 Firmware)

- 2503252_000047 (HP FutureSmart 5.3.2 Firmware)

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

**Table 1: TOE hardware and firmware reference**

| Product model name | Product number | System firmware version |
|---|---|---|
| HP LaserJet Enterprise MFP M430f | 3PZ55A | 2503252_000047 |
| HP LaserJet Enterprise MFP M431f | 3PZ56A | |
| HP LaserJet Managed MFP E42540f | 3PZ75A | |
| HP Color LaserJet Enterprise MFP M480f | 3QA55A | 2503252_000044 |
| HP Color LaserJet Managed MFP E47528f | 3QA75A | |

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

**Table 2: TOE English-guidance documentation reference**

| Models | Title | Reference |
|---|---|---|
| All models | Common Criteria Evaluated Configuration Guide for HP Multifunction Printers<br><br>HP Color LaserJet Enterprise MFP M480<br>HP Color LaserJet Managed MFP E47528<br>HP LaserJet Enterprise MFP M430/M431<br>HP LaserJet Managed MFP E42540<br><br>Edition 1, 5/2023 | [CCECG] |
| M430f, M431f | HP LaserJet Enterprise MFP M430, M431<br><br>User Guide<br><br>Edition 2, 2/2021 | [M430-31_UG] |
| M480f | HP Color LaserJet Enterprise MFP M480<br><br>User Guide<br><br>Edition 2, 2/2021 | [M480-UG] |
| E42540f | HP LaserJet Managed MFP E42540<br><br>User Guide<br><br>Edition 2, 2/2021 | [E42540_UG] |

| Models | Title | Reference |
|---|---|---|
| E47528f | HP Color LaserJet Managed MFP E47528<br><br>User Guide<br><br>Edition 2, 2/2021 | [E47528_UG] |
| M430f,<br>M431f,<br>M480f | HP LaserJet Enterprise MFP M430, M431<br>HP Color LaserJet Enterprise MFP M480<br><br>Installation Guide<br><br>2020 | [M430-31-480_IG] |
| E42540f<br>E47528f | HP LaserJet Managed MFP E42540<br>HP Color LaserJet Managed MFP E47528<br><br>Installation Guide<br><br>2020 | [M42540-47528_IG] |

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

**Table 3: TOE OS and processor**

| Item | Type |
|---|---|
| OS | Linux 4.9.180 |
| Processor | ARM Cortex-A72 |

## 1.5.2 TOE Architecture

The TOE is designed to be shared by many client computers and human users. It performs the functions of printing, copying, scanning, faxing, and storing/retrieving of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, to an analog telephone line using its internal analog fax modem, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration 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. These exclusions include paper/media trays and feeders, document feeders, output bins, and printer stands.

***Operating system and processor***

The TOE's operating system is Linux 4.9.180 running on an ARM Cortex-A72 processor.

***Networking***

The TOE supports Local Area Network (LAN) capabilities. The LAN is used to communicate with client computers, the administrative computer, and several trusted IT entities. Some TOE models include support for Wireless LAN (WLAN), but the WLAN must be disabled in the evaluated configuration.

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) 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.

***REST Web Services***

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

***Administrative Computer and Network Client Computers***

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. All other client computers connecting to the TOE to perform non-administrative tasks are known as Network Client Computers in this ST.

Network Client Computers connect to the TOE to submit print jobs to the TOE using the Printer Job Language (PJL) interface. They can also receive job status from the TOE using PJL. The PJL interface connection is protected using IPsec.

The [CCECG] section *IPsec* describes how to properly configure the TOE to allow a single Administrative Computer and one or more Network Client Computers.

***PSTN***

Some models of the TOE contain a built-in PSTN connection for sending and receiving faxes. For models of the TOE that do not have built-in analog fax functionality, an optional analog fax accessory can be installed to add analog fax functionality. The Control Panel uses identification and authentication to control access for sending faxes over PSTN.

***PJL***

The PJL interface is used by unauthenticated users via Network Client Computers to submit print jobs and receive job status (e.g., view the print queue). The unauthenticated users use PJL over an IPsec connection. It is also used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL over IPsec to send print jobs to the TOE as well as to receive job status. In general, PJL supports password-protected

administrative commands, but in the evaluated configuration, these commands are disabled. For the purposes of this Security Target, we define the PJL interface as PJL data sent to port 9100.

***SharePoint, FTP, and SMB***

The TOE supports Microsoft SharePoint 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, email received faxes, or email sent faxes. In addition, the TOE can send email alert messages to administrator-specified email addresses, mobile devices, or to a website.

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 and a physical home screen button 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 device. This storage device is an eMMC.

The disk drive contains a section called Job Storage which is a user-visible file system where user document data, such as stored print, stored copy, and stored received faxes, are located.

***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 these network-related features. 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 to the print jobs.

## 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)

#### 1.5.3.2.1 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), Digital Signature Algorithm (DSA), 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. 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.

#### 1.5.3.2.2 Storage Encryption

The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an eMMC. The TOE performs encryption of User Document Data and confidential TSF data on the eMMC without any user intervention.

*Customer Data Encryption*

The TSF implements a feature called Customer Data Encryption that is based on the device-mapper crypt (dm-crypt) target. dm-crypt provides transparent encryption of block devices using the HP FutureSmart Firmware Linux Kernel Crypto API. The Customer Data Encryption feature encrypts customer data (including User Document Data) stored on the partition (a.k.a., customer data partition) designated for storing customer data on the eMMC drive. In the evaluated configuration, the Customer Data Encryption feature is configured to use AES-CBC-256 to encrypt data.

Data stored on the customer data partition includes: Stored jobs (e.g., print, copy, fax), temporary job files, PJL and PostScript filesystem files including downloaded fonts, and extensibility customer data (if stored there by the extensibility solution).

*Certificate Data Encryption*

The TSF encrypts identity certificates and their corresponding private keys stored on the eMMC drive.

Certificates XML file:

The TSF stores the network identity certificate and its corresponding private key in encrypted form in a certificates XML file stored on the eMMC drive. AES-CBC-256 is used to encrypt the network identity certificate and its private key contained in the certificates XML file.

Thumbprint files:

The TSF stores identity certificates and their corresponding private keys in individual files (a.k.a., thumbprint files) stored in encrypted form on the eMMC drive. AES-CBC-256 is used to encrypt thumbprint files.

*JDI Configuration File Encryption*

The TSF encrypts the JDI configuration file which contains the IPsec pre-shared keys and other networking configuration data. The JDI configuration file is stored the eMMC drive and is encrypted using AES-CBC-256.

#### 1.5.3.2.3 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.

#### 1.5.3.2.4 Digital Signatures for TSF Testing

The TOE uses digital signatures as part of its TSF testing functionality. This is described in Section 1.5.3.8.

#### 1.5.3.2.5 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.

**Table 4: TOE cryptographic implementations**

| Cryptographic implementation | Usage |
|---|---|
| HP FutureSmart Firmware OpenSSL 1.1.1 | Storage Encryption, TSF Testing, Trusted Update |
| HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | IKE |
| HP FutureSmart Firmware Linux Kernel Crypto API | IPsec, Storage Encryption |

The product contains one eMMC drive (a.k.a., storage drive). The TOE encrypts specific areas of the storage drive containing customer data using AES-128-CBC. This can be configured to use AES-256-CBC encryption, if desired.

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 PJL interface does not appear in this table because the PJL interface does not perform authentication of users.

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.

***PJL user***

A user of the PJL network interface, used for submitting print jobs from a client computer.

***REST user***

A user of the REST network interface.

**Table 5: TOE authentication mechanisms and their supported interfaces**

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

#### 1.5.3.3.1 Internal Authentication

##### 1.5.3.3.1.1 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.

#### 1.5.3.3.2 External Authentication

##### 1.5.3.3.2.1 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.

##### 1.5.3.3.2.2 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.

#### 1.5.3.3.3 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., print, copy, fax) 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.

#### 1.5.3.3.4 Network Interface I&A

The EWS, PJL, and REST interfaces are network protocols protected by IPsec. The EWS and REST interfaces support one or more authentication mechanisms. These interfaces perform their I&A after the IPsec connection has been established. The PJL interface is an unauthenticated interface (i.e., it does not perform I&A).

##### 1.5.3.3.4.1 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.

##### 1.5.3.3.4.2 REST I&A

The REST 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 allows the following TSF-medicated actions prior to the REST I&A:

- Discover a subset of the Web Services
- Obtain X.509v3 certificate associated with the print engine

- Obtain configuration settings of the print engine
- Obtain list of installed licenses
- Install a digitally signed license
- Delete a license (if the license in the payload of the request is digitally signed)
- Obtain Web Services registration status
- Obtain printer Claim Code for Web Services registration
- Set printer Claim Code for Web Services registration

#### 1.5.3.3.5 Authentication Failure Handling and Authentication Feedback

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

- Control Panel
- EWS
- REST

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 storage device is an eMMC. The TSF ensures that confidential TSF Data and User Document Data stored on the drive is not stored as plaintext.

### 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 client computers. 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 a user authenticated using an External Authentication mechanism (Windows Sign In and LDAP Sign In), the roles are implemented as permission sets. In the case of a user authenticated using an Internal Authentication mechanism (Local Device 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 firmware files that have not been tampered with are loaded into memory. The TOE supports dm-verity to protect the integrity of the SquashFS file system firmware images. On each boot, the TOE verifies the digital signature of the dm-verity hash tree corresponding to a SquashFS file system firmware image. During operation, dm-verity verifies the integrity of a file system block before loading it into memory. The TOE uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to verify the integrity of a dm-verity hash tree. For additional details, see the TSS for FPT_TST_EXT.1.

#### 1.5.3.8 PSTN Fax-network Separation

The PSTN fax capability is either included with or can be added to the TOE. In either case, the TOE provides a distinct separation between the fax capabilities and the Ethernet network connection of the TOE prohibiting communication via the fax interface except when transmitting or receiving User Data using fax protocols. This is explained in more detail along with the fax capabilities in the TSS for FDP_FXS_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. Options and add-ons that are not security relevant, such as finishers, are not part of the evaluation but can be added to the TOE without any security implications.

Optional wireless add-ons are excluded from the TOE and are not part of the evaluation. Built-in wireless capabilities are disabled in the evaluated configuration.

Some TOE models come with built-in PSTN fax capabilities and some TOE models have this as an option. For TOE models where the PSTN fax is an option, the models can be used with or without the PSTN fax option.

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 file. 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—paper trays, document feeders, and output bins—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.
- Third-party solutions must not be installed on the TOE.
- PC Fax Send must be disabled.
- Fax polling receive must be disabled.
- Device USB must be disabled.
- Host USB plug and play must be disabled.
- Firmware upgrades through any means other than the EWS (e.g., PJL) and USB must be disabled.
- All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password.
- HP Jetdirect XML Services must be disabled.
- External file system access through PJL and PS must be disabled.
- Only X.509v3 certificates and pre-shared key are supported methods for IPsec authentication (IPsec authentication using Kerberos is not supported).
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Mandatory Sign-in must be enabled (this disables the Guest role).
- SNMP must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to support personnel, must be disabled.
- Wireless functionality must be disabled:
    - Near Field Communication (NFC) must be disabled.
    - Bluetooth Low Energy (BLE) must be disabled.
    - Wireless Direct Print must be disabled.
    - Wireless station must be disabled.
- PJL device access commands must be disabled.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the built-in Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS) using IPsec:
    - Open Extensibility Platform device (OXPd) Web Services
    - WS* Web Services

- Device Administrator Password must be set.
- Remote Configuration Password must not be set.
- OAUTH2 use is disallowed.
- SNMP over HTTP use is disallowed.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- All received faxes must be converted into stored faxes.
- Fax Archive must be disabled.
- Fax Forwarding must be disabled.
- Internet Fax and LAN Fax must be disabled.
- Firmware updates through REST Web Services is disallowed.
- Remote User Auto Capture must be disabled.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- Smart Cloud Print must be disabled.
- Partial Clean function must not be performed.

# 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.

**Table 6: NIAP TDs**

| NIAP TD | TD description | Applicability | TD reference |
|---|---|---|---|
| TD0157 | FCS_IPSEC_EXT.1.1 - Testing SPDs | Applicable. The TOE includes IPsec. | [CCEVS-TD0157] |
| TD0176 | FDP_DSK_EXT.1.2 - SED Testing | Not applicable. The TOE performs encryption in accordance with FCS_COP.1(d) | [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] |
| TD0393 | Require FTP_TRP.1(b) only for printing | Not applicable. The TOE supports a remote, non-administrative interface for submitting print jobs to the TOE. FTP_TRP.1(b) is claimed. | [CCEVS-TD0393] |

| NIAP TD | TD description | Applicability | TD reference |
|---|---|---|---|
| TD0474 | Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 | Not applicable. FCS_TLS_EXT.1 is not claimed. | [CCEVS-TD0474] |
| TD0494 | Removal of Mandatory SSH Ciphersuite for HCD | Not applicable. FCS_SSH_EXT.1.7 is not claimed. | [CCEVS-TD0494] |
| TD0562 | Test activity for Public Key Algorithms | Not applicable. FCS_SSH_EXT.1.5 is not claimed. | [CCEVS-TD0562] |
| TD0642 | FCS_CKM.1.1(a) and FCS_COP.1.1(b) Requirements in HCD PP v1.0 | Applicable. | [CCEVS-TD0642] |

# 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 of [HCDPP].

***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

**Table 7: Threats countered by the TOE**

| Threat | Description |
|---|---|
| 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. |

| Threat | Description |
|---|---|
| T.TSF_FAILURE | A malfunction of the TSF may cause loss of security if the TOE is permitted to operate while in a degraded state. |
| 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

**Table 8: Physical assumptions**

| Assumption | Description |
|---|---|
| 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

**Table 9: Personnel assumptions**

| Assumption | Description |
|---|---|
| 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

**Table 10: Connectivity assumptions**

| Assumption | Description |
|---|---|
| A.NETWORK | The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface. |

## 3.3 Organizational Security Policies

**Table 11: Organizational security policies**

| Organizational security policy | Description |
|---|---|
| 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.FAX_FLOW | If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN. |

# 4 Security Objectives

## 4.1 Objectives for the TOE

**Table 12: Security objectives for the TOE**

| Security objective | Description |
|---|---|
| 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.FAX_NET_SEPARATION | If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function. |

## 4.2 Objectives for the Operational Environment

**Table 13: Security objectives for the operational environment**

| Security objective | Description |
|---|---|
| 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.

**Table 14: Mapping of security objectives to threats and policies**

| Objective | Threats/OSPs |
|---|---|
| O.USER_I&A | T.UNAUTHORIZED_ACCESS<br>T.TSF_COMPROMISE<br>P.AUTHORIZATION |
| O.ACCESS_CONTROL | T.UNAUTHORIZED_ACCESS<br>T.TSF_COMPROMISE<br>P.AUDIT |
| O.USER_AUTHORIZATION | P.AUTHORIZATION<br>P.AUDIT |
| O.ADMIN_ROLES | T.UNAUTHORIZED_ACCESS<br>T.TSF_COMPROMISE<br>P.AUTHORIZATION |
| O.UPDATE_VERIFICATION | T.UNAUTHORIZED_UPDATE |

| Objective | Threats/OSPs |
|---|---|
| O.TSF_SELF_TEST | T.TSF_FAILURE |
| O.COMMS_PROTECTION | T.NET_COMPROMISE<br>P.COMMS_PROTECTION |
| O.AUDIT | P.AUDIT |
| O.STORAGE_ENCRYPTION | P.STORAGE_ENCRYPTION |
| O.KEY_MATERIAL | P.KEY_MATERIAL |
| O.FAX_NET_SEPARATION | P.FAX_FLOW |

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

**Table 15: Mapping of security objectives for the Operational Environment to assumptions, threats and policies**

| 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 |

## 4.3.2 Sufficiency

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

**Table 16: Sufficiency of objectives countering threats**

| Threat | Rationale for security objectives |
|---|---|
| T.UNAUTHORIZED_ACCESS | O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users.<br>O.USER_I&A provides the basis for access control.<br>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. |

| Threat | Rationale for security objectives |
|---|---|
| | O.USER_I&A provides the basis for access control.<br>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. |

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

**Table 17: Sufficiency of objectives holding assumptions**

| 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.<br>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. |

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.

**Table 18: Sufficiency of objectives enforcing Organizational Security Policies**

| OSP | Rationale for security objectives |
|---|---|
| P.AUTHORIZATION | O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users.<br>O.USER_I&A provides the basis for authorization. |

| OSP | Rationale for security objectives |
|---|---|
| | O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators. |
| P.AUDIT | O.AUDIT requires the generation of audit data.<br>O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users.<br>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.FAX_FLOW | O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN. |

# 5 Extended Components Definition

All 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<br>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.<br><br>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 Cryptographic Key Management (FCS_CKM)

#### Family behaviour

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

#### Component levelling

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

#### 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<br>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.<br>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 Key Derivation

# Family behaviour

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

# Component levelling

FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

# Management: FCS_KDF_EXT.1

There are no management activities foreseen.

# Audit: FCS_KDF_EXT.1

There are no audit events foreseen.

### 5.2.3.1 FCS_KDF_EXT.1 – Cryptographic Key Derivation

Hierarchical to: No other components

Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),

[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

**FCS_KDF_EXT.1.1** The TSF shall accept [selection: a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask] to derive an intermediate key, as defined in [selection: NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

## 5.2.4 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.

### 5.2.4.1 FCS_KYC_EXT.1 – Extended: Key Chaining

Hierarchical to: No other components

Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping), FCS_SMC_EXT.1 Extended: Submask Combining, FCS_COP.1(i) Cryptographic operation (Key Transport), FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)]

**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 wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, 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.

## 5.2.5 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.

### 5.2.5.1 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.<br><br>This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component. |

## 5.2.6 Extended: Submask Combining

### Family behaviour

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

### Component levelling

FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion.

### Management: FCS_SMC_EXT.1

There are no management activities foreseen.

### Audit: FCS_SMC_EXT.1

There are no audit events foreseen.

#### 5.2.6.1 FCS_SMC_EXT.1 – Extended: Submask Combining

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | FCS_COP.1(c) Cryptographic operation (Hash Algorithm) |
| **FCS_SMC_EXT.1.1** | The TSF shall combine submasks using the following method [selection: exclusive OR (XOR), SHA-256, SHA-512] to generate an intermediary key or BEV. |
| Rationale | Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.<br><br>This extended component protects the TSF data using cryptographic algorithms, 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.<br>This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component. |

## 5.3.2 Extended: Fax Separation (FDP_FXS)

# Family behaviour

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

# Component levelling

FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

# Management: FDP_FXS_EXT.1

There are no management activities foreseen.

## Audit: FDP_FXS_EXT.1

There are no audit events foreseen.

#### 5.3.2.1 FDP_FXS_EXT.1 – Extended: Fax Separation

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| **FDP_FXS_EXT.1.1** | The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols. |
| Rationale | Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.<br>This extended component protects the TSF Data or User Data, 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: **"!", "@", "#", "$", "%", "^", "&", "*", "(", ")" , [assignment: other characters]**];

- 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.<br><br>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.<br><br>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.<br>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.<br><br>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.).

**Table 19: Security functional requirements for the TOE**

| Security functional group | Security functional requirement | Base security functional component | Source | Operations | | | |
|---|---|---|---|---|---|---|---|
| | | | | Iter. | Ref. | Ass. | Sel. |
| FAU - Security audit | FAU_GEN.1 Audit data generation | | 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 | Yes | Yes | 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 | No | No | Yes |
| | FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption) | FCS_COP.1 | HCDPP | Yes | No | No | Yes |

| Security functional group | Security functional requirement | Base security functional component | Source | Operations | | | |
|---|---|---|---|---|---|---|---|
| | | | | Iter. | Ref. | Ass. | Sel. |
| | FCS_COP.1(f) Cryptographic operation (Key Encryption) | FCS_COP.1 | HCDPP | Yes | No | No | Yes |
| | FCS_COP.1(g) Cryptographic operation (for keyed-hash message authentication) | FCS_COP.1 | HCDPP | Yes | Yes | Yes | Yes |
| | FCS_COP.1(h) Cryptographic operation (for keyed-hash message authentication) | FCS_COP.1 | HCDPP | Yes | No | No | Yes |
| | FCS_IPSEC_EXT.1 Extended: IPsec selected | | HCDPP | No | No | Yes | Yes |
| | FCS_KDF_EXT.1 | | HCDPP | No | No | No | Yes |
| | FCS_KYC_EXT.1/CDE Extended: Key chaining | FCS_KYC_EXT.1 | HCDPP | Yes | No | No | Yes |
| | FCS_KYC_EXT.1/CM Extended: Key chaining | FCS_KYC_EXT.1 | HCDPP | Yes | No | No | Yes |
| | FCS_KYC_EXT.1/CMT Extended: Key chaining | FCS_KYC_EXT.1 | HCDPP | Yes | No | No | Yes |
| | FCS_KYC_EXT.1/JCF Extended: Key chaining | FCS_KYC_EXT.1 | HCDPP | Yes | No | No | Yes |
| | FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation) | | HCDPP | No | Yes | Yes | Yes |
| | FCS_SMC_EXT.1/JCF Extended: Submask Combining | FCS_SMC_EXT.1 | HCDPP | Yes | No | No | Yes |
| | FCS_SMC_EXT.1/CMT Extended: Submask Combining | FCS_SMC_EXT.1 | HCDPP | Yes | No | No | 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 |

| Security functional group | Security functional requirement | Base security functional component | Source | Operations | | | |
|---|---|---|---|---|---|---|---|
| | | | | Iter. | Ref. | Ass. | Sel. |
| | FDP_DSK_EXT.1 Extended: Protection of Data on Disk | | HCDPP | No | No | No | Yes |
| | FDP_FXS_EXT.1 Extended: Fax separation | | HCDPP | No | 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 | No | Yes | Yes |
| | FIA_PSK_EXT.1 Extended: Pre-shared key composition | | HCDPP | No | No | Yes | Yes |
| | FIA_UAU.1 Timing of authentication | | HCDPP | No | No | Yes | No |
| | 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 | Yes | 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 | Yes | Yes | No |
| | FMT_SMR.1 Security roles | | HCDPP | No | No | No | No |

| Security functional group | Security functional requirement | Base security functional component | Source | Operations | | | |
|---|---|---|---|---|---|---|---|
| | | | | Iter. | Ref. | Ass. | Sel. |
| 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 |
| 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 |
| | FTP_TRP.1(b) Trusted path (for Non-administrators) | FTP_TRP.1 | HCDPP | Yes | No | No | Yes |

## 6.1.1 Security audit (FAU)

### 6.1.1.1 Audit data generation (FAU_GEN.1)

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All auditable events specified in Table 20, **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 20, **none**.

**Table 20: Auditable events**

| Auditable event | Relevant SFR(s) | Additional information | Origin |
|---|---|---|---|
| Job completion | FDP_ACF.1 | Type of job | [HCDPP] |
| Unsuccessful user authentication | FIA_UAU.1 | Required by [HCDPP]:<br>• None | [HCDPP] |
| Unsuccessful user identification | FIA_UID.1 | Required by [HCDPP]:<br>• None<br>Added by vendor:<br>• The attempted user identity | [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]:<br>• None<br>Added by vendor:<br>• New date and time<br>• Old date and time | [HCDPP] |
| Failure to establish session | FTP_ITC.1<br>FTP_TRP.1(a)<br>FTP_TRP.1(b) | Required by [HCDPP]:<br>• Reason for failure<br>Added by vendor:<br>• 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 |

**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 (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**

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

**Table 21: Asymmetric key generation**

| Usage | Implementation | Purpose | Algorithm | Key sizes | Related SFRs |
|---|---|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | KAS FFC | DH (dhEphem) | P=2048, SHA2-256 | FCS_COP.1(c)<br>FCS_IPSEC_EXT.1<br>FCS_RBG_EXT.1 |
| | | | DSA | L=2048, N=224;<br>L=2048, N=256;<br>L=3072, N=256 | |

**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 22*** that meet the following: No Standard.

**Table 22: Symmetric key generation**

| Usage | Implementation | Purpose | Key sizes | Related SFRs |
|---|---|---|---|---|
| Storage encryption | HP FutureSmart Firmware OpenSSL 1.1.1 | Key generation for Customer Data Encryption | 256 bits | FCS_KYC_EXT.1/CDE<br>FCS_RBG_EXT.1 |
| | | Key generation for certificate data encryption | 256 bits | FCS_KYC_EXT.1/CM<br>FCS_KYC_EXT.1/CMT<br>FCS_RBG_EXT.1 |

| Usage | Implementation | Purpose | Key sizes | Related SFRs |
|---|---|---|---|---|
| | | Key generation for JDI configuration file encryption | 256 bits | FCS_KYC_EXT.1/JCF FCS_RBG_EXT.1 |

**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(a)** 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 23** and cryptographic key sizes 128-bits and 256-bits that meets the following:

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

**Table 23: AES encryption/decryption algorithms**

| Usage | Implementation | Purpose | Algorithm | Modes | Key sizes | Related SFRs |
|---|---|---|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | Data encryption and decryption | AES | CBC | 128 bits, 256 bits | FCS_IPSEC_EXT.1 |
| | | Encryption in CTR_DRBG(AES) | AES | ECB | 256 bits | |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | Data encryption and decryption | AES | CBC | 128 bits, 256 bits | FCS_IPSEC_EXT.1 |

**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 24**

that meets the following

**Case: RSA Digital Signature Algorithm**

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

**Table 24: Asymmetric algorithms for signature generation/verification**

| Usage | Implementation | Purpose | Algorithm | Key sizes | Related SFRs |
|---|---|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | Signature generation and verification based on PKCS#1 v1.5 | RSA | 2048 bits, 3072 bits | FCS_IPSEC_EXT.1 |
| Trusted update | HP FutureSmart Firmware OpenSSL 1.1.1 | Signature verification based on PKCS#1 v1.5 | RSA | 2048 bits | FPT_TUD_EXT.1 |
| TSF testing | HP FutureSmart Firmware OpenSSL 1.1.1 | Signature verification based on PKCS#1 v1.5 | RSA | 2048 bits | FPT_TST_EXT.1 |

**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 25** that meet the following: [ISO/IEC 10118-3:2004].

**Table 25: Hash algorithms**

| Usage | Implementation | Purpose | Algorithm | Related SFRs |
|---|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 | Pre-shared keys | SHA-1, SHA2-256, SHA2-512 | FIA_PSK_EXT.1 |
| | | KAS FFC | SHA2-256 | FCS_CKM.1(a) |

| Usage | Implementation | Purpose | Algorithm | Related SFRs |
|---|---|---|---|---|
| | Cryptographic Module | 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 | SHA2-256, SHA2-384, SHA2-512 | FCS_COP.1(g) |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | HMAC | SHA-1, SHA2-256, SHA2-384, SHA2-512 | FCS_COP.1(g) |
| | | HMAC (HMAC_DRBG) | SHA-2-256 | FCS_COP.1(g)<br>FCS_RBG_EXT.1 |
| Trusted update | HP FutureSmart Firmware OpenSSL 1.1.1 | RSA digital signature verification | SHA2-256 | FPT_TUD_EXT.1 |
| TSF testing | HP FutureSmart Firmware OpenSSL 1.1.1 | RSA digital signature verification | SHA2-256 | FPT_TST_EXT.1 |
| Storage encryption | HP FutureSmart Firmware OpenSSL 1.1.1 | HMAC (PBKDF2) | SHA2-256 | FDP_DSK_EXT.1<br>FCS_KDF_EXT.1 |
| | | Submask combining | SHA2-256 | FDP_DSK_EXT.1<br>FCS_SMC_EXT.1/JCF |

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

### 6.1.2.8 Cryptographic operation (AES Data Encryption/Decryption) (FCS_COP.1(d))

**FCS_COP.1.1(d)** The TSF shall perform data encryption and decryption in accordance with a specified cryptographic algorithm ***defined in Table 26*** and cryptographic key sizes ***defined in Table 26*** that meet the following: **AES as specified in ISO/IEC 18033-3**, **CBC as specified in ISO/IEC 10116**.

**Table 26: AES encryption/decryption algorithms**

| Usage | Implementation | Purpose | Algorithm | Key size | Related SFRs |
|---|---|---|---|---|---|
| Storage encryption | HP FutureSmart Firmware Linux Kernel Crypto API | Customer data encryption and decryption | AES-CBC-256 | 256 bits | FDP_DSK_EXT.1 |
| | HP FutureSmart Firmware OpenSSL 1.1.1 | Certificate data and JDI configuration file encryption and decryption | AES-CBC-256 | 256 bits | FDP_DSK_EXT.1 |
| | | CTR_DRBG(AES) | AES-EBC-256 | 256 bits | FDP_DSK_EXT.1 FCS_CKM.1(b) |

**TSS Link**: *TSS for FCS_COP.1(d)*.

### 6.1.2.9 Cryptographic operation (Key Encryption) (FCS_COP.1(f))

**FCS_COP.1.1(f)** The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm ***defined in Table 27*** and cryptographic key sizes ***defined in Table 27*** that meet the following: AES as specified in ISO /IEC 18033-3, CBC as specified in ISO/IEC 10116.

**Table 27: Key encryption**

| Usage | Implementation | Purpose | Algorithm | Key size | Related SFRs |
|---|---|---|---|---|---|
| Storage encryption | HP FutureSmart Firmware Linux Kernel Crypto API | Encryption/ decryption of volume key (dm-crypt) | AES-CBC-256 | 256 bits | FCS_KYC_EXT.1/CDE |

**TSS Link**: *TSS for FCS_COP.1(f)*.

### 6.1.2.10 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 28***, key size ***defined in Table 28*** and message digest sizes ***defined in Table 28 in*** bits that meet the following: FIPS PUB 198-1, 'The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."'

**Table 28: HMAC algorithms**

| Usage | Implementation | Algorithm | Key size | Digest size | Related SFRs |
|---|---|---|---|---|---|
| IKE | | HMAC-SHA2-256-128 | 256 bits | 256 bits | FCS_IPSEC_EXT.1 |

| Usage | Implementation | Algorithm | Key size | Digest size | Related SFRs |
|---|---|---|---|---|---|
| | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | HMAC-SHA2-384-192 | 384 bits | 384 bits | |
| | | HMAC-SHA2-512-256 | 512 bits | 512 bits | |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | HMAC-SHA1-96 | 160 bits | 160 bits | FCS_IPSEC_EXT.1 |
| | | HMAC-SHA2-256-128 | 256 bits | 256 bits | |
| | | HMAC-SHA2-384-192 | 384 bits | 384 bits | |
| | | HMAC-SHA2-512-256 | 512 bits | 512 bits | |

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

### 6.1.2.11 Cryptographic operation (for keyed-hash message authentication) (FCS_COP.1(h)

**FCS_COP.1.1(h)** The TSF shall perform **keyed-hash message authentication** in accordance with **HMAC-SHA-256** and cryptographic key sizes **256 bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”; ISO/IEC 10118.

**TSS Link**: *TSS for FCS_COP.1(h)*.

### 6.1.2.12 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*.

### 6.1.2.13 Extended: Cryptographic Key Derivation (FCS_KDF_EXT.1)

**FCS_KDF_EXT.1.1** The TSF shall accept **a RNG generated submask as specified in FCS_RBG_EXT.1** to derive an intermediate key, as defined in **NIST SP 800-132**, using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

**TSS Link**: *TSS for FCS_KDF_EXT.1*.

### 6.1.2.14 Extended: Key chaining (FCS_KYC_EXT.1/CDE)

**FCS_KYC_EXT.1.1** The TSF shall maintain a key chain of: **intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): key derivation as specified in FCS_KDF_EXT.1; key encryption as specified in FCS_COP.1(f)** while maintaining an effective strength of **256 bits**.

**TSS Link**: *TSS for FCS_KYC_EXT.1/CDE*.

### 6.1.2.15 Extended: Key chaining (FCS_KYC_EXT.1/CM)

**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/CM*.

### 6.1.2.16 Extended: Key chaining (FCS_KYC_EXT.1/CMT)

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

**TSS Link**: *TSS for FCS_KYC_EXT.1/CMT*.

### 6.1.2.17 Extended: Key chaining (FCS_KYC_EXT.1/JCF)

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

**TSS Link**: *TSS for FCS_KYC_EXT.1/JCF*.

### 6.1.2.18 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 29***.

**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 29 of hardware-based noise source(s)** with a minimum of ***bits defined in Table 29*** 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.

**Table 29: DRBG algorithms**

| Usage | Implementation | Algorithm | Hardware noise sources | Minimum entropy bits | Related SFRs |
|---|---|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | CTR_DRBG(AES) | 1 | 256 bits | FCS_CKM.1(a)<br>FCS_COP.1(a)<br>FCS_IPSEC_EXT.1 |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | HMAC_DRBG (HMAC-SHA2-256) | 1 | 256 bits | FCS_CKM.1(a)<br>FCS_COP.1(g)<br>FCS_IPSEC_EXT.1 |
| Storage encryption | HP FutureSmart Firmware OpenSSL 1.1.1 | CTR_DRBG(AES) | 1 | 256 bits | FCS_CKM.1(b)<br>FCS_COP.1(a)<br>FDP_DSK_EXT.1 |

**TSS Link**: *TSS for FCS_RBG_EXT.1*.

### 6.1.2.19 Extended: Submask Combining (FCS_SMC_EXT.1/JCF)

**FCS_SMC_EXT.1.1** The TSF shall combine submasks using the following method **exclusive OR (XOR), SHA-256** to generate an intermediary key or BEV.

**TSS Link**: *TSS for FCS_SCM_EXT.1/JCF*.

### 6.1.2.20 Extended: Submask Combining (FCS_SMC_EXT.1/CMT)

**FCS_SMC_EXT.1.1** The TSF shall combine submasks using the following method **exclusive OR (XOR)** to generate an intermediary key or BEV.

**TSS Link**: *TSS for FCS_SCM_EXT.1/CMT*.

## 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 28 and Table 29.

**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 30 and Table 31.

**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 30 and Table 31.

**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**.

**Table 30: D.USER.DOC Access Control SFP**

| | | **"Create"** | **"Read"** | **"Modify"** | **"Delete"** |
|---|---|---|---|---|---|
| **Print** | ***Operation:*** | ***Submit a document to be printed*** | ***View image or Release printed output*** | ***Modify stored document*** | ***Delete stored document*** |
| | **Job owner** | **n/a** | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **n/a** | **denied** | **denied by design** | **allowed** |
| | **U.NORMAL** | **n/a** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **allowed** | **denied** | **denied by design** | **denied** |
| **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 by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Copy** | ***Operation:*** | ***Submit a document for copying*** | ***View scanned image or Release printed copy output*** | ***Modify stored image*** | ***Delete stored image*** |
| | **Job owner** | **allowed** | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **denied** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Fax send** | ***Operation:*** | ***Submit a document to send as a fax*** | ***View scanned image*** | ***Modify stored image*** | ***Delete stored image*** |
| | **Job owner** | **allowed** | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **denied** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Fax receive** | ***Operation:*** | ***Receive a fax and store it*** | ***View fax image or Release printed fax output*** | ***Modify image of received fax*** | ***Delete image of received fax*** |

| | | | | | |
|---|---|---|---|---|---|
| | **Fax owner** | **allowed** | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Storage/ retrieval** | ***Operation:*** | ***Store document*** | ***Retrieve stored document*** | ***Modify stored document*** | ***Delete stored document*** |
| | **Job owner** | **allowed** (note 1) | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | Fax: **allowed** Print: **denied** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **allowed** (condition 1) | **denied** | **denied by design** | **denied** |

**Table 31: D.USER.JOB Access Control SFP**

| | | **"Create"** | **"Read"** | **"Modify"** | **"Delete"** |
|---|---|---|---|---|---|
| **Print** | ***Operation:*** | ***Create print job*** | ***View print queue / log*** | ***Modify print job*** | ***Cancel print job*** |
| | **Job owner** | **n/a** | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **n/a** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **n/a** | Queue: **allowed** Log: **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **allowed** | **denied** | **denied by design** | **denied** |
| **Scan** | ***Operation:*** | ***Create scan job*** | ***View scan status / log*** | ***Modify scan job*** | ***Cancel scan job*** |
| | **Job owner** | **allowed** (note 2) | **allowed** | **denied by design** | **allowed** |

| | | | | | |
|---|---|---|---|---|---|
| | **U.ADMIN** | **denied** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | Status: **allowed**<br>Log: **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Copy** | ***Operation:*** | ***Create copy job*** | ***View copy status / log*** | ***Modify copy job*** | ***Cancel copy job*** |
| | **Job owner** | **allowed**<br>(note 2) | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | Status: **allowed**<br>Log: **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Fax send** | ***Operation:*** | ***Create fax job*** | ***View fax job queue / log*** | ***Modify fax send job*** | ***Cancel fax send job*** |
| | **Job owner** | **allowed**<br>(note 2) | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | Queue: **allowed**<br>Log: **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Fax receive** | ***Operation:*** | ***Create fax job*** | ***View fax receive status / log*** | ***Modify fax receive job*** | ***Cancel fax receive job*** |
| | **Fax owner** | **allowed**<br>(note 3) | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied**<br>(note 4) | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied**<br>(note 4) | Status: **allowed**<br>Log: **denied** | **denied by design** | **denied** |

| | | | | | |
|---|---|---|---|---|---|
| | **Unauthenticated** | **denied** | **denied** | **denied by design** | **denied** |
| **Storage/ retrieval** | ***Operation:*** | ***Create storage / retrieval job*** | ***View storage / retrieval log*** | ***Modify storage / retrieval job*** | ***Cancel storage / retrieval job*** |
| | **Job owner** | **allowed** (note 1) | **allowed** | **denied by design** | **allowed** |
| | **U.ADMIN** | **denied** | **allowed** | **denied by design** | **allowed** |
| | **U.NORMAL** | **denied** | **denied** | **denied by design** | **denied** |
| | **Unauthenticated** | **allowed** (condition 1) | **denied** | **denied by design** | **denied** |

**TSS Link**: *TSS for FDP_ACF.1*.

**HCDPP Application Note**: The term "n/a" means not applicable.

**Condition 1**: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

**Note 1**: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.

**Note 2**: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.

**Note 3**: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.

**Note 4**: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.

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

**FDP_DSK_EXT.1.1** The TSF shall **perform encryption in accordance with FCS_COP.1(d)**, 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 Extended: Fax separation (FDP_FXS_EXT.1)

**FDP_FXS_EXT.1.1** The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

**TSS Link**: *TSS for FDP_FXS_EXT.1*.

## 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 REST**
  - **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)**
- **REST 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)**

**Application Note**: PJL users are unauthenticated.

**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 REST 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:**
  - **View the Welcome message**
  - **Reset the session**
  - **Select the Sign In button**
  - **Select a sign-in method from Sign In screen**
  - **View the device status information**
  - **Change the display language for the session**
  - **Place the device into sleep mode**
  - **View or print network connectivity status information**
  - **View or print Web Services status information**

- **View help information**
- **View the system time**

- **EWS:**
  - **Select a sign in method**
- **REST:**
  - **Discover a subset of the Web Services**
  - **Obtain the X.509v3 certificate on the print engine**
  - **Obtain the secure configuration settings on the print engine**
  - **Obtain list of installed licenses**
  - **Install a digitally signed license**
  - **Delete a license (if the license in the payload of the request is digitally signed)**
  - **Obtain Web Services registration status**
  - **Obtain printer Claim Code for Web Services registration**
  - **Set printer Claim Code for Web Services registration**

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:**
  - **View the Welcome message**
  - **Reset the session**
  - **Select the Sign In button**
  - **Select a sign-in method from Sign In screen**
  - **View the device status information**
  - **Change the display language for the session**
  - **Place the device into sleep mode**
  - **View or print network connectivity status information**
  - **View or print Web Services status information**
  - **View help information**
  - **View the system time**
- **EWS:**

- **Select a sign-in method**

- **REST:**
  - **Discover a subset of the Web Services**
  - **Obtain the X.509v3 certificate on the print engine**
  - **Obtain the secure configuration settings on the print engine**
  - **Obtain list of installed licenses**
  - **Install a license if the license in the payload of the request is digitally signed**
  - **Delete a license if the license in the payload of the request is digitally signed**
  - **Obtain Web Services registration status**
  - **Obtain printer Claim Code for Web Services registration**
  - **Set printer Claim Code for Web Services registration**

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
   - REST 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
   - REST 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 32 on*** the functions **defined in Table 32** to U.ADMIN.

**Table 32: Management of functions**

| 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 Mandatory Sign-in | Enable, disable | FIA_ATD.1<br>FIA_UAU.1<br>FIA_UID.1 | In the evaluated configuration, the "Control Panel Mandatory Sign-in" 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. |

| Function | Actions | Related SFRs | Application note |
|---|---|---|---|
| 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. |
| Enhanced security event logging | Enable, disable | FAU_GEN.1 | In the evaluated configuration, enhanced security event logging must be enabled. |
| 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. |

**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 33 on** the security attributes **defined in Table 33** to **the authorized identified roles defined in Table 33**.

**Table 33: Management of security attributes**

| 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 |

| TOE component | Security attribute | Available operations | Restricted operations | Authorized identified roles | Default value property | Default value override roles |
|---|---|---|---|---|---|---|
| | 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 |
| Job Storage object attributes | Job owner | View | View | Job owner, U.ADMIN | n/a | No role |
| | Fax owner | View | View | U.ADMIN | Restrictive | No role |

**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 t**he properties defined in Table 33 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 33*** to 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 34**.

**Table 34: Management of TSF Data**

| 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 |

| Data | Operation | Authorized roles | Related SFR(s) |
|---|---|---|---|
| Permission set associations (except on the Device Administrator account) | Add, delete, view | U.ADMIN | FDP_ACF.1<br>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 |
| NTS server configuration data | Change | U.ADMIN | FPT_STM.1 |
| 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 |

**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 35**.

**Table 35: Specification of management functions**

| Management function | SFR | TSS page number | Objectives |
|---|---|---|---|
| Management of Device Administrator password | FMT_MTD.1 | 154 | O.USER_AUTHORIZATION, O.USER_I&A |
| Management of account lockout policy | FMT_MTD.1 | 154 | O.USER_I&A |
| Management of minimum length password settings | FMT_MTD.1 | 154 | |
| Management of Internal and External authentication mechanisms | FMT_MOF.1 | 150 | |
| Management of "Allow users to choose alternate sign-in methods at the product control panel" function | FMT_MOF.1 | 150 | |
| Management of session inactivity timeouts | FMT_MTD.1 | 154 | |

| Management function | SFR | TSS page number | Objectives |
|---|---|---|---|
| Management of permission set associations | FMT_MTD.1 | 154 | O.ADMIN_ROLES |
| Management of permission set permissions | FMT_MSA.1 | 152 | O.ACCESS_CONTROL |
| Management of IPsec pre-shared keys | FMT_MTD.1 | 154 | O.COMMS_PROTECTION |
| Management of CA and identity certificates for IPsec authentication | FMT_MTD.1 | 154 | |
| Management of enhanced security event logging | FMT_MOF.1 | 150 | O.AUDIT |
| Management of NTS configuration data | FMT_MTD.1 | 154 | |

**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/CDE, FCS_KYC_EXT.1/CM, FCS_KYC_EXT.1/CMT, and FCS_KYC_EXT.1/JCF 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)*.

### 6.1.8.3 Trusted path (for Non-administrators) (FTP_TRP.1(b))

**FTP_TRP.1.1(b)** The TSF shall use **IPsec** to provide a trusted communication path between itself and remote users 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(b)** The TSF shall permit **remote users** to initiate communication via the trusted path.

**FTP_TRP.1.3(b)** The TSF shall require the use of the trusted path for initial user authentication and all remote user actions.

**TSS Link**: *TSS for FTP_TRP.1(b)*.

## 6.2 Security Functional Requirements Rationale

## 6.2.1 Coverage

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

**Table 36: Mapping of security functional requirements to security objectives**

| 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 |

| Security functional requirements | Objectives |
|---|---|
| FCS_CKM.1(b) | O.COMMS_PROTECTION<br>O.STORAGE_ENCRYPTION |
| FCS_CKM_EXT.4 | O.COMMS_PROTECTION<br>O.STORAGE_ENCRYPTION |
| FCS_CKM.4 | O.COMMS_PROTECTION<br>O.STORAGE_ENCRYPTION |
| FCS_COP.1(a) | O.COMMS_PROTECTION |
| FCS_COP.1(b) | O.COMMS_PROTECTION<br>O.UPDATE_VERIFICATION |
| FCS_COP.1(c) | O.COMMS_PROTECTION<br>O.STORAGE_ENCRYPTION<br>O.UPDATE_VERIFICATION |
| FCS_COP.1(d) | O.STORAGE_ENCRYPTION |
| FCS_COP.1(f) | O.STORAGE_ENCRYPTION |
| FCS_COP.1(g) | O.COMMS_PROTECTION |
| FCS_COP.1(h) | O.STORAGE_ENCRYPTION |
| FCS_IPSEC_EXT.1 | O.COMMS_PROTECTION |
| FCS_KDF_EXT.1 | O.STORAGE_ENCRYPTION |
| FCS_KYC_EXT.1/CDE | O.STORAGE_ENCRYPTION |
| FCS_KYC_EXT.1/CM | O.STORAGE_ENCRYPTION |
| FCS_KYC_EXT.1/CMT | O.STORAGE_ENCRYPTION |
| FCS_KYC_EXT.1/JCF | O.STORAGE_ENCRYPTION |
| FCS_RBG_EXT.1 | O.COMMS_PROTECTION<br>O.STORAGE_ENCRYPTION |
| FCS_SMC_EXT.1/JCF | O.STORAGE_ENCRYPTION |
| FCS_SMC_EXT.1/CMT | O.STORAGE_ENCRYPTION |
| FDP_ACC.1 | O.ACCESS_CONTROL<br>O.USER_AUTHORIZATION |
| FDP_ACF.1 | O.ACCESS_CONTROL<br>O.USER_AUTHORIZATION |

| Security functional requirements | Objectives |
|---|---|
| FDP_DSK_EXT.1 | O.STORAGE_ENCRYPTION |
| FDP_FXS_EXT.1 | O.FAX_NET_SEPARATION |
| 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,<br>O.USER_I&A |
| FIA_USB.1 | O.USER_I&A |
| FMT_MOF.1 | O.ADMIN_ROLES |
| FMT_MSA.1 | O.ACCESS_CONTROL,<br>O.USER_AUTHORIZATION |
| FMT_MSA.3 | O.ACCESS_CONTROL,<br>O.USER_AUTHORIZATION |
| FMT_MTD.1 | O.ACCESS_CONTROL |
| FMT_SMF.1 | O.ACCESS_CONTROL,<br>O.ADMIN_ROLES,<br>O.USER_AUTHORIZATION |
| FMT_SMR.1 | O.ACCESS_CONTROL,<br>O.ADMIN_ROLES,<br>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 |

| Security functional requirements | Objectives |
|---|---|
| FTP_ITC.1 | O.AUDIT<br>O.COMMS_PROTECTION |
| FTP_TRP.1(a) | O.COMMS_PROTECTION |
| FTP_TRP.1(b) | O.COMMS_PROTECTION |

## 6.2.2 Sufficiency

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

**Table 37: Security objectives for the TOE rationale**

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| O.USER_I&A | FIA_AFL.1 | Supports | This SFR protects the authentication function by limiting the number of unauthorized authentication attempts that can be made, thereby reducing the likelihood of impersonation. |
| | FIA_PMG_EXT.1 | Satisfies | This SFR protects the authentication function by providing for strong credentials that are difficult to guess or derive. |
| | FIA_UAU.1 | Satisfies | This SFR defines the TOE functions that can be performed without authentication and the functions that require authentication for use. |
| | FIA_UAU.7 | Satisfies | This SFR protects the authentication function by hiding the authentication credential as it is being input. |
| | FIA_UID.1 | Satisfies | This SFR defines the TOE functions that can be performed without identification and the functions that require identification for use. |
| | FIA_USB.1 | Satisfies | 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. |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| | FTA_SSL.3 | Satisfies | This SFR helps prevent User or Administrator impersonation by terminating unattended sessions. |
| O.ACCESS_CONTROL | FDP_ACC.1 | Satisfies | This SFR defines the access control policy that is used to protect access to User Data and TSF Data. |
| | FDP_ACF.1 | Satisfies | 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." |
| | FMT_MSA.1 | Supports | 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. |
| | FMT_MSA.3 | Supports | |
| | FMT_MTD.1 | Supports | |
| | FMT_SMF.1 | Supports | |
| | FMT_SMR.1 | Supports | |
| O.USER_AUTHORIZATION | FDP_ACC.1 | Supports | This SFR enforces User Access Control SFP on subjects, objects, and operations in accordance with user authorization. |
| | FDP_ACF.1 | Supports | This SFR enforces the User Access Control SFP to objects based on attributes in accordance with user authorization. |
| | FIA_ATD.1 | Supports | This SFR defines the attributes that are associated with Users that can be used to define their authorizations. |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| | FMT_MSA.1 | Satisfies | This SFR defines the authorizations that are required to access data that is protected by the TSF. |
| | FMT_MSA.3 | Satisfies | 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. |
| | FMT_SMF.1 | Satisfies | This SFR defines the management functions provided by the TOE that can be used to define User authorizations. |
| | FMT_SMR.1 | Satisfies | This SFR defines administrative roles that can be used to define authorizations to groups of Users. |
| O.ADMIN_ROLES | FIA_UID.1 | Supports | This SFR defines the TOE management functions that can be accessed without requiring Administrator authorization. |
| | FMT_MOF.1 | Satisfies | This SFR defines the authorizations that are required for Administrators to access TOE functions. |
| | FMT_SMF.1 | Satisfies | This SFR defines the administrative functions that are provided by the TSF. |
| | FMT_SMR.1 | Satisfies | This SFR defines the different roles that can be assigned to Administrators for the purposes of determining authentication and authorization. |
| O.UPDATE_VERIFICATION | FCS_COP.1(b) | Selection | This SFR defines the digital signature service(s) used to verify the authenticity TOE updates. |
| | FCS_COP.1(c) | Selection | This SFR defines the hashing algorithm(s) used to verify the integrity of TOE updates. |
| | FPT_TUD_EXT.1 | Satisfies | This SFR defines the ability of the TOE to be updated and the method(s) by which the updates are known to be trusted. |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| O.TSF_SELF_TEST | FPT_TST_EXT.1 | Satisfies | This SFR defines the ability of the TSF to perform self-tests which assert the security properties of the TOE. |
| O.COMMS_PROTECTION | FCS_CKM.1(a) | Satisfies | This SFR defines the use of secure algorithms for key pair generation that can be used for key transport during protected communications. |
| | FCS_CKM.1(b) | Satisfies | This SFR defines the use of secure algorithms for key generation that can be used for protected communications. |
| | FCS_CKM.4 | Supports | 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. |
| | FCS_CKM_EXT.4 | Supports | This SFR ensures that residual cryptographic data cannot be used to compromise protected communications. |
| | FCS_COP.1(a) | Satisfies | This SFR defines the use of a secure symmetric key algorithm that can be used for protected communications. |
| | FCS_COP.1(b) | Satisfies | This SFR defines the digital signature services(s) used for protected communications. |
| | FCS_COP.1(c) | Selection | 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. |
| | FCS_COP.1(g) | Satisfies | This SFR defines the use of a secure HMAC algorithm that can be used for protected communications. |
| | FCS_IPSEC_EXT.1 | Selection | This SFR defines secure communications protocols that can be used to protect the transmission of security-relevant data. |
| | FCS_RBG_EXT.1 | Supports | This SFR supports protected communications by defining a secure method of random bit generation that |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| | | | allows cryptographic functions to operate with their theoretical maximum strengths. |
| | FIA_PSK_EXT.1 | Selection | This SFR defines the use of pre-shared keys in IPsec which allows for the secure implementation of that protocol. |
| | FPT_SKP_EXT.1 | Satisfies | This SFR prevents the compromise of protected communications by ensuring that secret cryptographic data is protected against unauthorized access. |
| | FTP_ITC.1 | Satisfies | This SFR defines the interfaces over which protected communications are required and the methods used to protect the communications used to transit those interfaces. |
| | FTP_TRP.1(a) | Satisfies | This SFR defines the protected communications path that is used to secure Administrator interaction with the TOE. |
| | FTP_TRP.1(b) | Satisfies | This SFR defines the protected communications path that is used to secure user interaction with the TOE. |
| O.AUDIT | FAU_GEN.1 | Satisfies | This SFR defines the auditable events for which the TOE generates audit data and the fields that are included in each audit record. |
| | FAU_GEN.2 | Satisfies | This SFR defines the ability of the TOE to apply attribution to all activities performed by a user or Administrator. |
| | FAU_STG_EXT.1 | Satisfies | This SFR defines the ability of the TSF to transmit generated audit data to an external entity using a protected channel. |
| | FPT_STM.1 | Supports | This SFR ensures that audit data is labeled with accurate timestamps. |
| | FTP_ITC.1 | Supports | This SFR defines the protected communications channel(s) over which audit data can be transmitted. |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| O.STORAGE_ENCRYPTION | FCS_CKM.1(b) | Selection | This SFR defines the use of secure algorithms for key generation that can be used for storage encryption. |
| | FCS_CKM.4 | Supports | This SFR defines the method used by the TOE to destroy cryptographic keys used for customer data and certificate data encryption. |
| | FCS_CKM_EXT.4 | Supports | 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. |
| | FCS_COP.1(c) | Supports | This SFR defines the hashing services used by the TOE when deriving the Key Encryption Key (KEK) for customer data encryption and submask combining for JDI configuration file encryption. |
| | FCS_COP.1(d) | Supports | This SFR defines the encryption/decryption algorithm used by the TOE to encrypt/decrypt User Document Data and confidential TSF Data stored on the Field-Replaceable Nonvolatile Storage Device. |
| | FCS_COP.1(f) | Supports | This SFR defines the encryption/decryption algorithms used by the TOE to encrypt/decrypt the volume key used for storage encryption. |
| | FCS_COP.1(h) | Option | This SFR defines the keyed-hash message authentication used by the TOE when deriving the Key Encryption Key (KEK) for customer data encryption. |
| | FCS_KDF_EXT.1 | Option | This SFR defines the key derivation function used by the TOE for derivation of the Key Encryption Key (KEK) used for customer data encryption. |
| | FCS_KYC_EXT.1/CDE | Satisfies | This SFR defines the key chaining method used by the TOE for customer |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| | | | data encryption to provide multiple layers of security for key material. |
| | FCS_KYC_EXT.1/CM | Satisfies | This SFR defines the key chaining method used by the TOE for certificate data encryption to provide multiple layers of security for key material. |
| | FCS_KYC_EXT.1/CMT | Satisfies | This SFR defines the key chaining method used by the TOE for certificate data encryption to provide multiple layers of security for key material. |
| | FCS_KYC_EXT.1/JCF | Satisfies | This SFR defines the key chaining method used by the TOE for JDI configuration file encryption to provide multiple layers of security for key material. |
| | FCS_RBG_EXT.1 | Supports | This SFR supports storage encryption by defining the random bit generation algorithm used to ensure that the TOE's cryptographic algorithms function with the theoretical maximum level of security. |
| | FCS_SMC_EXT.1/JCF | Selection | This SFR defines the submask combining used by the TOE to generate the intermediate key used for encrypting/decrypting the JDI configuration file. |
| | FCS_SMC_EXT.1/CMT | Selection | This SFR defines the submask combining used by the TOE to generate the data encryption key used to encrypt/decrypt identity certificates and their private key blobs. |
| | FDP_DSK_EXT.1 | Satisfies | This SFR requires the TSF to encrypt the data that is stored to disk. |
| O.KEY_MATERIAL | FPT_KYP_EXT.1 | Satisfies | This SFR defines the ability of the TSF from storing unprotected key data in insecure locations. |
| O.FAX_NET_SEPARATION | FDP_FXS_EXT.1 | Satisfies | This SFR enforces separation of the fax interface by preventing the use of this |

| Security objectives | SFR | Relationship | Rationale |
|---|---|---|---|
| | | | interface for all non-fax communications. |

## 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.

**Table 38: TOE SFR dependency analysis**

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 | FPT_STM.1 | FPT_STM.1 |
| FAU_GEN.2 | FAU_GEN.1 | FAU_GEN.1 | Not applicable | FAU_GEN.1 |
| | FIA_UID.1 | FIA_UID.1 | Not applicable | FIA_UID.1 |
| FAU_STG_EXT.1 | Not applicable | FAU_GEN.1 | Not applicable | FAU_GEN.1 |
| | Not applicable | FTP_ITC.1 | Not applicable | FTP_ITC.1 |
| FCS_CKM.1(a) | [FCS_CKM.2 or FCS_COP.1] | [~~FCS_CKM.2, or~~ FCS_COP.1(b)] | [~~FCS_CKM.2, or~~ FCS_COP.1(b)~~]~~ FCS_COP.1(i)] | FCS_COP.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 |
| FCS_CKM.1(b) | [FCS_CKM.2 or FCS_COP.1] | [~~FCS_CKM.2, or~~ FCS_COP.1(f)] | [~~FCS_CKM.2, or~~ FCS_COP.1(a) FCS_COP.1(d) FCS_COP.1(e) FCS_COP.1(f)~~]~~ FCS_COP.1(g) FCS_COP.1(h)] | FCS_COP.1(f) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| | Not applicable | FCS_RBG_EXT.1 | FCS_RBG_EXT.1 | FCS_RBG_EXT.1 |
| FCS_CKM_EXT.4 | Not applicable | FCS_CKM.1(a) or FCS_CKM.1(b) | FCS_CKM.1(a) or FCS_CKM.1(b) | FCS_CKM.1(a) FCS_CKM.1(b) |
| | Not applicable | FCS_CKM.4 | FCS_CKM.4 | FCS_CKM.4 |
| FCS_CKM.4 | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | FCS_CKM.1(a) or FCS_CKM.1(b) | FCS_CKM.1(a) or FCS_CKM.1(b) | FCS_CKM.1(a) FCS_CKM.1(b) |
| FCS_COP.1(a) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or~~ FCS_CKM.1(b)] | Not applicable | FCS_CKM.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | Not applicable | FCS_CKM_EXT.4 |
| FCS_COP.1(b) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1~~] | [~~FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1~~ FCS_CKM.1(a)] | 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 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 |
| FCS_COP.1(c) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | No dependencies | Not applicable | This dependency has been removed by the PP. |
| | FCS_CKM.4 | No dependencies | Not applicable | This dependency has been removed by the PP. |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| FCS_COP.1(d) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or~~ FCS_CKM.1(b)] | Not applicable | FCS_CKM.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | Not applicable | FCS_CKM_EXT.4 |
| FCS_COP.1(f) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or~~ FCS_CKM.1(b)] | Not applicable | FCS_CKM.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | Not applicable | FCS_CKM_EXT.4 |
| FCS_COP.1(g) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or~~ FCS_CKM.1(b)] | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1(b)] | FCS_CKM.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 |
| FCS_COP.1(h) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | [~~FDP_ITC.1, or FDP_ITC.2, or~~ FCS_CKM.1(b)] | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1(b)] | FCS_CKM.1(b) |
| | FCS_CKM.4 | Not applicable | Not applicable | This dependency has been removed by the PP. |
| | Not applicable | FCS_COP.1(c) | FCS_COP.1(c) | FCS_COP.1(c) |
| | Not applicable | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 | FCS_CKM_EXT.4 |
| FCS_IPSEC_EXT.1 | Not applicable | Not applicable | FCS_CKM.1(a) | FCS_CKM.1(a) |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| | Not applicable | FCS_COP.1(g) | FCS_COP.1(a)<br>FCS_COP.1(b)<br>FCS_COP.1(c)<br>FCS_COP.1(g) | FCS_COP.1(a)<br>FCS_COP.1(b)<br>FCS_COP.1(c)<br>FCS_COP.1(g) |
| | Not applicable | Not applicable | FCS_RBG_EXT.1 | FCS_RBG_EXT.1 |
| | Not applicable | FIA_PSK_EXT.1 | FIA_PSK_EXT.1 | FIA_PSK_EXT.1 |
| FCS_KDF_EXT.1 | Not applicable | FCS_COP.1(h) | FCS_COP.1(h) | FCS_COP.1(h) |
| | Not applicable | FCS_RBG_EXT.1 | FCS_RBG_EXT.1 | FCS_RBG_EXT.1 |
| FCS_KYC_EXT.1/CDE | Not applicable | FCS_COP.1(e) | Not applicable | FCS_COP.1(e) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(i) | Not applicable | FCS_COP.1(i) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(f) | Not applicable | FCS_COP.1(f) |
| | Not applicable | FCS_KDF_EXT.1 | Not applicable | FCS_KDF_EXT.1 |
| | Not applicable | FCS_SMC_EXT.1 | Not applicable | FCS_SMC_EXT.1 is not an item selected in FCS_KYC_EXT.1/CDE. |
| FCS_KYC_EXT.1/CM | Not applicable | FCS_COP.1(e) | Not applicable | FCS_COP.1(e) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(i) | Not applicable | FCS_COP.1(i) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| | Not applicable | FCS_COP.1(f) | Not applicable | FCS_COP.1(f) is not an item selected in FCS_KYC_EXT.1/CM. |
| | Not applicable | FCS_KDF_EXT.1 | Not applicable | FCS_KDF_EXT.1 is not an item selected in FCS_KYC_EXT.1/CM. |
| | Not applicable | FCS_SMC_EXT.1 | Not applicable | FCS_SMC_EXT.1 is not an item selected in FCS_KYC_EXT.1/CM. |
| FCS_KYC_EXT.1/CMT | Not applicable | FCS_COP.1(e) | Not applicable | FCS_COP.1(e) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(i) | Not applicable | FCS_COP.1(i) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(f) | Not applicable | FCS_COP.1(f) is not an item selected in FCS_KYC_EXT.1/CMT. |
| | Not applicable | FCS_KDF_EXT.1 | Not applicable | FCS_KDF_EXT.1 is not an item selected in FCS_KYC_EXT.1/CMT. |
| | Not applicable | FCS_SMC_EXT.1 | Not applicable | FCS_SMC_EXT.1 |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| FCS_KYC_EXT.1/JCF | Not applicable | FCS_COP.1(e) | Not applicable | FCS_COP.1(e) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(i) | Not applicable | FCS_COP.1(i) is excluded from the ST. See Section 6.2.4 for exclusion rationale. |
| | Not applicable | FCS_COP.1(f) | Not applicable | FCS_COP.1(f) is not an item selected in FCS_KYC_EXT.1/JCF. |
| | Not applicable | FCS_KDF_EXT.1 | Not applicable | FCS_KDF_EXT.1 is not an item selected in FCS_KYC_EXT.1/JCF. |
| | Not applicable | FCS_SMC_EXT.1 | Not applicable | FCS_SMC_EXT.1 |
| FCS_RBG_EXT.1 | Not applicable | No dependencies | Not applicable | |
| FCS_SMC_EXT.1/JCF | Not applicable | FCS_COP.1(c) | Not applicable | FCS_COP.1(c) |
| FCS_SMC_EXT.1/CMT | Not applicable | FCS_COP.1(c) | Not applicable | FCS_COP.1(c) |
| FDP_ACC.1 | FDP_ACF.1 | FDP_ACF.1 | Not applicable | FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1 | FDP_ACC.1 | Not applicable | FDP_ACC.1 |
| | FMT_MSA.3 | FMT_MSA.3 | Not applicable | FMT_MSA.3 |
| FDP_DSK_EXT.1 | Not applicable | FCS_COP.1(d) | Not applicable | FCS_COP.1(d) |
| FDP_FXS_EXT.1 | Not applicable | No dependencies | Not applicable | |
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.1 | Not applicable | FIA_UAU.1 |
| FIA_ATD.1 | No dependencies | No dependencies | Not applicable | |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| FIA_PMG_EXT.1 | Not applicable | No dependencies | Not applicable | |
| FIA_PSK_EXT.1 | Not applicable | FCS_RBG_EXT.1 | Not applicable | FCS_RBG_EXT.1 |
| FIA_UAU.1 | FIA_UID.1 | FIA_UID.1 | Not applicable | FIA_UID.1 |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.1 | Not applicable | FIA_UAU.1 |
| FIA_UID.1 | No dependencies | No dependencies | Not applicable | |
| FIA_USB.1 | FIA_ATD.1 | FIA_ATD.1 | Not applicable | FIA_ATD.1 |
| FMT_MOF.1 | FMT_SMR.1 | FMT_SMR.1 | Not applicable | FMT_SMR.1 |
| | FMT_SMF.1 | FMT_SMF.1 | Not applicable | FMT_SMF.1 |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1] | [FDP_ACC.1, ~~or FDP_IFC.1~~] | Not applicable | FDP_ACC.1 |
| | FMT_SMR.1 | FMT_SMR.1 | Not applicable | FMT_SMR.1 |
| | FMT_SMF.1 | FMT_SMF.1 | Not applicable | FMT_SMF.1 |
| FMT_MSA.3 | FMT_MSA.1 | FMT_MSA.1 | Not applicable | FMT_MSA.1 |
| | FMT_SMR.1 | FMT_SMR.1 | Not applicable | FMT_SMR.1 |
| FMT_MTD.1 | FMT_SMR.1 | FMT_SMR.1 | FMT_SMR.1 | FMT_SMR.1 |
| | FMT_SMF.1 | FMT_SMF.1 | FMT_SMF.1 | FMT_SMF.1 |
| FMT_SMF.1 | No dependencies | No dependencies | No dependencies | |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 | Not applicable | FIA_UID.1 |
| FPT_KYP_EXT.1 | Not applicable | No dependencies | No dependencies | |
| FPT_SKP_EXT.1 | Not applicable | No dependencies | Not applicable | |
| FPT_STM.1 | No dependencies | No dependencies | Not applicable | |
| FPT_TST_EXT.1 | Not applicable | No dependencies | Not applicable | |
| FPT_TUD_EXT.1 | Not applicable | [FCS_COP.1(b), or FCS_COP.1(c)] | ~~[~~FCS_COP.1(b), ~~or~~ FCS_COP.1(c)~~]~~. | FCS_COP.1(b) FCS_COP.1(c) |
| FTA_SSL.3 | No dependencies | No dependencies | Not applicable | |

| Security functional requirement | Dependencies CC Part 2 | Dependencies HCDPP | Dependencies HCDPP Errata | Resolution |
|---|---|---|---|---|
| FTP_ITC.1 | No dependencies | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | FCS_IPSEC_EXT.1 |
| FTP_TRP.1(a) | No dependencies | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | FCS_IPSEC_EXT.1 |
| FTP_TRP.1(b) | No dependencies | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | [FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1] | FCS_IPSEC_EXT.1 |

### 6.2.4 HCDPP SFR reconciliation

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

**Table 39: HCDPP SFRs excluded from the ST**

| 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(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. |
| 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. |

| Excluded PP SFR | Type | Rationale |
|---|---|---|
| FCS_HTTPS_EXT.1 | Selection-based | All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information. |
| 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_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. |
| FDP_RIP.1(a) | Optional | O.IMAGE_OVERWRITE is not supported in the evaluated configuration. |
| FDP_RIP.1(b) | Optional | O.PURGE_DATA is not supported in the evaluated configuration. |

## 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.).

**Table 40: Security assurance requirements**

| 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 |

| Security assurance class | Security assurance requirement | Source | Operations | | | |
|---|---|---|---|---|---|---|
| | | | Iter. | Ref. | Ass. | Sel. |
| | 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 |
| 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 |

## 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 41 provide a quick index to each SFR's TSS entry in Table 42 of the next section.

**Table 41: TSS index**

| SFR | TSS page | SFR | TSS page | SFR | TSS page | SFR | TSS page |
|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | 100 | FCS_IPSEC_EXT.1 | 122 | FIA_ATD.1 | 140 | FPT_STM.1 | 159 |
| FAU_GEN.2 | 106 | FCS_KDF_EXT.1 | 126 | FIA_PMG_EXT.1 | 141 | FPT_TST_EXT.1 | 159 |
| FAU_STG_EXT.1 | 106 | FCS_KYC_EXT.1/ CDE | 127 | FIA_PSK_EXT.1 | 141 | FPT_TUD_EXT.1 | 160 |
| FCS_CKM.1(a) | 108 | FCS_KYC_EXT.1/ CM | 127 | FIA_UAU.1 | 142 | FTA_SSL.3 | 161 |
| FCS_CKM.1(b) | 109 | FCS_KYC_EXT.1/ CMT | 128 | FIA_UAU.7 | 146 | FTP_ITC.1 | 161 |
| FCS_CKM_EXT.4 | 110 | FCS_KYC_EXT.1/ JCF | 129 | FIA_UID.1 | 147 | FTP_TRP.1(a) | 162 |
| FCS_CKM.4 | 110 | FCS_RBG_EXT.1 | 129 | FMT_MOF.1 | 150 | FTP_TRP.1(b) | 163 |
| FCS_COP.1(a) | 115 | FCS_SMC_EXT.1/ JCF | 130 | FMT_MSA.1 | 152 | | |
| FCS_COP.1(b) | 115 | FCS_SMC_EXT.1/ CMT | 131 | FMT_MSA.3 | 154 | | |
| FCS_COP.1(c) | 116 | FDP_ACC.1 | 131 | FMT_MTD.1 | 154 | | |
| FCS_COP.1(d) | 119 | FDP_ACF.1 | 131 | FMT_SMF.1 | 156 | | |
| FCS_COP.1(f) | 120 | FDP_DSK_EXT.1 | 135 | FMT_SMR.1 | 156 | | |
| FCS_COP.1(g) | 120 | FDP_FXS_EXT.1 | 137 | FPT_KYP_EXT.1 | 158 | | |
| FCS_COP.1(h) | 121 | FIA_AFL.1 | 139 | FPT_SKP_EXT.1 | 158 | | |

### 7.1.1 TOE SFR compliance rationale

Table 42 provides the rationale for how the TOE complies with each of the SFRs in Section 6.1. Table 42 uses the following abbreviations.

- AA—Assurance Activity
- n/a—Not applicable
- Resp—Response

**Table 42: TOE SFR compliance rationale**

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | **Objective(s)**: O.AUDIT |

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td>FAU_GEN.1 (Audit generation)</td><td>
<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] in chapter 7 Enhanced security event logging messages in section Syslog messages. The [CCECG] groups the events into event categories in the section Syslog messages.
Table 43 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 43: TOE audit records
<table>
<tr><th>Auditable event</th><th>Additional information</th><th>CCECG “Syslog messages” category and records</th></tr>
<tr><td>Start-up and shutdown of the audit functions</td><td>None</td><td><u>Enhanced security event logging:</u><ul><li>Auditing was started during boot up</li><li>Auditing was stopped using EWS</li><li>Auditing was restarted using EWS</li></ul></td></tr>
<tr><td>Job completion</td><td>Type of job</td><td><u>Job completion:</u><ul><li>Copy job completion</li><li>Email job completion</li><li>Save (scan) to SharePoint job completion</li><li>Save (scan) to Network Folder job completion</li><li>Fax Send job completion</li></ul></td></tr>
</table>
</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | | |
|---|---|---|---|
| | | | • Fax Receive job completion<br>• Save to Device Memory job completion<br>• Retrieve from Device Memory job completion (Print from job storage)<br>• Job Notification completion<br>• Print job completion |
| | Unsuccessful user authentication | [HCDPP]:<br>• None | <u>Local device sign in:</u><br>• Local Device sign-in method failed |
| | | | <u>Windows sign in:</u><br>• Windows sign-in method failed for the specified user |
| | | | <u>LDAP sign in:</u><br>• LDAP sign-in method failed for the specified user |
| | Unsuccessful user identification | [HCDPP]:<br>• None<br>Vendor:<br>• Attempted user identity | Same categories and records as the "Unsuccessful user authentication" auditable events |
| | Use of the management functions | None | <u>Device administrator password:</u><br>• Device Administrator Password modified |
| | | | <u>Account lockout policy:</u> |

| TOE SFRs | TOE SFR compliance rationale | | |
|---|---|---|---|
| | | | • Account Lockout Policy enabled<br>• Account Lockout Policy disabled<br>• Account Lockout Policy setting modified |
| | | | Minimum password length settings:<br>• Minimum Password Length Policy setting modified |
| | | | Windows Sign In:<br>• Windows Sign In enabled<br>• Windows Sign In disabled<br>• Windows Sign In configuration modified |
| | | | LDAP Sign In:<br>• LDAP Sign In enabled<br>• LDAP Sign In disabled<br>• LDAP Sign In configuration modified |
| | | | "Allow users to choose alternate sign-in methods at the product control panel" function:<br>• Sign In and Permission Policy settings modified |

| TOE SFRs | TOE SFR compliance rationale | | |
|---|---|---|---|
| | | | Session inactivity timeout:<br>• Control Panel Inactivity Timeout Changed<br>• EWS Session Timeout modified |
| | | | Permission set associations:<br>• Default Permission set for sign-in method modified<br>• User to Permission Set Relationship added<br>• User to Permission Set Relationship deleted<br>• Group to Permission Set Relationship added<br>• Group to Permission Set Relationship deleted |
| | | | Custom permission sets:<br>• Permission Set added<br>• Permission Set modified<br>• Permission Set copied<br>• Permission Set deleted |
| | | | Permissions associated with permission sets:<br>• Permission Set modified |
| | | | IPsec pre-shared keys: |

| TOE SFRs | TOE SFR compliance rationale | | |
|---|---|---|---|
| | | | • IPsec policy added<br>• IPsec policy modified<br>• IPsec policy deleted |
| | | | <u>CA and identity certificates used for IPsec authentication:</u><br>• Device CA certificate installed<br>• Device CA certificate deleted<br>• Device Identity certificate and private key installed<br>• Device Identity certificate for network identity selected<br>• Device Identity certificate deleted |
| | | | <u>Enhanced security event logging:</u><br>• CCC logging started<br>• CCC logging stopped |
| | | | <u>NTS configuration data:</u><br>• Date and Time configuration modified |
| | Modifications to the group of users that are part of a role | None | <u>Network user to permission set relationships:</u><br>• User to Permission Set Relationship added |

| TOE SFRs | TOE SFR compliance rationale | | |
|---|---|---|---|
| | | | • User to Permission Set Relationship deleted |
| | | | Network group to permission set relationships:<br>• Group to Permission Set Relationship added<br>• Group to Permission Set Relationship deleted |
| | Changes to the time | [HCDPP]:<br>• None<br>Vendor:<br>• New date and time<br>• Old date and time | System time:<br>• System time changed |
| | Failure to establish session (trusted channel/path) | [HCDPP]:<br>• Reason for failure<br>Vendor:<br>• Non-TOE endpoint of connection (e.g., IP address) | IKEv1 phase 1 negotiations:<br>• IKEv1 phase 1 negotiation failed initiated by the client computer<br>• IKEv1 phase 1 negotiation failed initiated by the local device (TOE) |
| | | | IKEv1 phase 2 negotiations:<br>• IKEv1 phase 2 negotiation failed initiated by the client computer<br>• IKEv1 phase 2 negotiation failed initiated by the local device (TOE) |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">
<table>
<tr><td>Locking an account</td><td>User name associated with account</td><td><u>Account entered lockout (protected) mode:</u><ul><li>Account Entered Lockout Mode</li></ul></td></tr>
<tr><td>Unlocking an account</td><td>User name associated with account</td><td><u>Account exited lockout (protected) mode:</u><ul><li>Account Exited Lockout Mode</li></ul></td></tr>
</table>
</td></tr>
<tr><td></td><td>AA</td><td>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>Table 20 contains the auditable events for FAU_GEN.1. Table 41 contains the TSS auditable events and records.</td></tr>
<tr><td>FAU_GEN.2<br>(Audit user identification)</td><td colspan="2"><u>Objective(s)</u>: O.AUDIT<br><br><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>The Assurance Activities for FAU_GEN.1 address this SFR.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FAU_STG_EXT.1<br>(Audit trail storage)</td><td colspan="2"><u>Objective(s)</u>: O.AUDIT<br><br><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.<br><br>The TOE contains two in-memory audit record message queues. One queue is for network audit records (e.g., IKEv1 phase 1 negotiation events) 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.<br><br>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.<br><br>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 written to</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | the internal log file, then removed from the queue once the record has been successfully received by the syslog server.<br><br>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.<br><br>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.<br><br>**Note**: The TOE also stores up to 2500 audit records in an internal log file on the storage drive replacing the oldest audit records with new audit records when the log file becomes full. These audit records can be exported via the EWS interface. In the evaluated configuration, access to the audit records export function is restricted to U.ADMIN. | |
| | AA | *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.* |
| | Resp | The TOE uses the syslog protocol over an IPsec channel to transfer audit data to the external audit server. |
| | AA | *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.* |
| | Resp | 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) and written to the internal log file. Once an audit record is sent to the external syslog server, it is removed from the queue.<br><br>No TOE interface is provided to access the two in-memory queues; thus, no unauthorized access is possible.<br><br>Using the EWS interface, U.ADMIN can export the audit records in the internal log file. Access to the audit records export function is restricted to U.ADMIN. |

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td>FCS_CKM.1(a) (Asymmetric key generation)</td><td>
<u>Objective(s)</u>: O.COMMS_PROTECTION<br><br>
<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.<br><br>
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.<br>
• L=2048, N=224<br>
• L=2048, N=256<br>
• L=3072, N=256<br><br>
For KAS FFC, any necessary key material is obtained using the QuickSec 7.3 Cryptographic Module CTR_DRBG(AES) defined in FCS_RBG_EXT.1.<br><br>
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.<br><br>
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)<br><br>
Table 44: Asymmetric key generation
<table>
<tr><th>Usage</th><th>Implementation</th><th>Algorithm</th><th>Modes and key sizes</th></tr>
<tr><td rowspan="2">IKE</td><td rowspan="2">HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module</td><td>DH (dhEphem)</td><td>SHA2-256</td></tr>
<tr><td>DSA</td><td>L=2048, N=224;<br>L=2048, N=256;<br>L=3072, N=256</td></tr>
</table>
<table>
<tr><td>AA</td><td>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</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></td><td>implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.</td></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"><u>Objective(s)</u>: O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION<br><br><u>Summary</u>: The TOE uses the HP FutureSmart Firmware OpenSSL 1.1.1 CTR_DRBG(AES) defined in FCS_RBG_EXT.1 to generate keys used for storage encryption. Table 45 shows the purpose and key size of each key generated and the standards to which they conform. For information on how the TOE invokes the DRBG, see the [KMD].<br><br>Table 45: 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 rowspan="2">Storage encryption</td><td rowspan="2">HP FutureSmart Firmware OpenSSL 1.1.1</td><td>Passphrase and volume key generation (dm-crypt)</td><td>ARM Cortex-A72</td><td>256-bits</td><td>No standard</td></tr>
<tr><td>Data encryption key generation (certificate data encryption/decryption)</td><td>ARM Cortex-A72</td><td>256-bits</td><td>No standard</td></tr>
</table></td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Intermediate key generation (JDI configuration file encryption/decryption) | ARM Cortex-A72 | 256-bits | No standard |

| | |
|---|---|
| AA | *The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.* |
| Resp | This information is provided in the [KMD]. |

**FCS_CKM_EXT.4** (Key material destruction)

**Objective(s)**: O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION

**Summary**: The TOE's plaintext secret and private cryptographic keys and cryptographic critical security parameters (CSPs) are as follows.

- IPsec (for O.COMMS_PROTECTION):
  - IPsec keys and key material
- Customer Data Encryption (for O.STORAGE_ENCRYPTION):
  - Passphrase, derived key, and volume key
- JDI Configuration File Encryption (for O.STORAGE_ENCRYPTION):
  - Intermediate key, and data encryption key
- Certificate Data Encryption (for O.STORAGE_ENCRYPTION):
  - Certificates XML file:
    - Data encryption key
  - Thumbprint files:
    - Intermediate key
    - Data encryption key

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.

| | |
|---|---|
| AA | *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.* |
| Resp | TSS for FCS_CKM.4 contains the requested information on a per key basis. |

**FCS_CKM.4** (Key destruction)

**Objective(s)**: O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION

**Summary**: 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 (for O.COMMS_PROTECTION):

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | ○ IPsec keys and key material<br>• Customer Data Encryption (for O.STORAGE_ENCRYPTION):<br>○ Passphrase, derived key, and volume key<br>• JDI Configuration File Encryption (for O.STORAGE_ENCRYPTION):<br>○ Intermediate key, and data encryption key<br>• Certificate Data Encryption (for O.STORAGE_ENCRYPTION):<br>○ Certificates XML file:<br>▪ Data encryption key<br>○ Thumbprint files:<br>▪ Intermediate key<br>▪ Data encryption key<br><br>*Rationale for no nonvolatile key destruction*<br><br>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.<br>• Customer Data Encryption:<br>○ Passphrase — In the evaluated configuration, the passphrase is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified, thus, it is never destroyed.<br>○ Volume key — In the evaluated configuration, the volume key is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified, thus, it is never destroyed.<br>• JDI Configuration File Encryption:<br>○ Intermediate key — In the evaluated configuration, this key is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified, thus, it is never destroyed.<br>○<br>• Certificate Data Encryption:<br>○ Certificates XML file:<br>▪ Data encryption key — In the evaluated configuration, the data encryption key is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified, thus, it is never destroyed.<br>○ Thumbprint files:<br>▪ Intermediate key— In the evaluated configuration, this key is not viewable from the TOE interfaces by an administrator or non-administrator, and is never modified, thus, it is never destroyed.<br>• IPsec: |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|

- IPsec Pre-shared keys—The JDI configuration file contains the IPsec pre-shared keys and is stored on the eMMC drive. For additional information on how IPsec PSKs are protected, see the JDI Configuration File Encryption description above.
- IPsec RSA private key— When an identity certificate with private key is imported, the TSF stores the certificate and the private key in encrypted form on the eMMC drive. For additional information on how the RSA private key is protected, see Certificate Data Encryption above.

Table 46 contains the list of the volatile memory keys, their usage, their storage location, when they are no longer needed, when they are destroyed, and their destruction algorithm.

**Table 46: 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 |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 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 |
| Passphrase<br><br>(Customer Data Encryption) | Used as input into PBKDF2 to derive the derived key | RAM | After the derived key has been generated | Power off | Power loss |
| Derived key<br><br>(Customer Data Encryption) | Used to encrypt/decrypt the volume key | RAM | After volume key has been encrypted/ unencrypted | Power off | Power loss |

| TOE SFRs | TOE SFR compliance rationale | | | | | |
|---|---|---|---|---|---|---|
| | Volume key<br><br>(Customer Data Encryption) | Used to encrypt/decrypt data on customer data partition | RAM | Needed while the HCD is powered on | Power off | Power loss |
| | Intermediate key<br><br>(JDI configuration file encryption) | Combined with other data to generate the data encryption key | RAM | After the data encryption key has been generated | Power off | Power loss |
| | Data encryption key<br><br>(JDI configuration file encryption) | Used to encrypt/ decrypt the JDI configuration file | RAM | Needed while the HCD is powered on | Power off | Power loss |
| | Data encryption key<br><br>(Certificates XML file encryption) | Used to encrypt/ decrypt the certificates XML file | RAM | Needed while the HCD is powered on | Power off | Power loss |
| | Intermediate key<br><br>(Thumbprint file encryption) | Combined with a submask value to generate the data encryption key | RAM | After the data encryption key has been generated | Power off | Power loss |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Data encryption key<br><br>(Thumbprint file encryption) | Used to encrypt/decrypt thumbprint files containing identity certificates and their corresponding private keys | RAM | Needed while the HCD is powered on | Power off | Power loss |

| | |
|---|---|
| AA | *The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.* |
| Resp | The Summary section above contains the requested information on a per key basis. |

FCS_COP.1(a) (AES)

**Objective(s)**: O.COMMS_PROTECTION

**Summary**: IKE and IPsec support both AES CBC 128-bit and AES CBC 256-bit for symmetric data encryption and decryption.

IKE supports AES ECB 256-bit for the symmetric encryption in CTR_DRBG(AES) using the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module meeting both [FIPS197] and [SP800-38A] standards.

**Table 47: AES algorithms**

| Usage | Implementation | Algorithm | Modes and key sizes |
|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | AES encryption and decryption | AES-CBC-128, AES-CBC-256 |
| | | AES encryption | AES-ECB-256 |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | AES encryption and decryption | AES-CBC-128, AES-CBC-256 |

| | |
|---|---|
| AA | *None* |
| Resp | n/a |

FCS_COP.1(b) (RSA)

**Objective(s)**: O.COMMS_PROTECTION, O.UPDATE_VERIFICATION

**Summary**: The TOE's IKE uses RSA certificates for digital signature-based authentication. IKE uses the RSA 2048-bit and 3072-bit algorithms for digital signature authentication (i.e., signature generation and verification) using the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module. The RSA signature generation is based on PKCS#1 v1.5 and uses

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
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 IKE, see the TSS for FCS_IPSEC_EXT.1.<br><br>
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 Firmware OpenSSL 1.1.1 implementation of the RSA 2048-bit algorithm. For more details on trusted update, see the TSS for FPT_TUD_EXT.1.<br><br>
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 Firmware OpenSSL 1.1.1 implementation of the RSA 2048-bit algorithm. For more details on TSF testing, see the TSS for FPT_TST_EXT.1.<br><br>
All implementations meet the [FIPS186-4] standard.<br><br>
Table 48: Asymmetric algorithms for signature generation/verification
<table>
<tr><th>Usage</th><th>Implementation</th><th>Algorithm</th><th>Key sizes</th></tr>
<tr><td rowspan="2">IKE</td><td rowspan="2">HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module</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></tr>
<tr><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></tr>
<tr><td>Trusted update</td><td>HP FutureSmart Firmware OpenSSL 1.1.1</td><td>RSA signature verification based on PKCS#1 v1.5 using SHA2-256</td><td>2048-bits</td></tr>
<tr><td>TSF testing</td><td>HP FutureSmart Firmware OpenSSL 1.1.1</td><td>RSA signature verification based on PKCS#1 v1.5 using SHA2-256</td><td>2048-bits</td></tr>
</table>
<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><u>Objective(s)</u>:<br>• O.COMMS_PROTECTION<br>• O.UPDATE_VERIFICATION</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | • O.STORAGE_ENCRYPTION<br><br>**Summary**:<br><br>*IKE*<br><br>IKE 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.<br><br>IKE supports SHA2-256 for KAS FFC as specified in FCS_CKM.1(a).<br><br>IKE 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).<br><br>Also, IKE supports HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 which use SHA-1, SHA2-256, SHA2-384, and SHA2-512, respectively.<br><br>IKE uses the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module 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).<br><br>*IPsec*<br><br>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.<br><br>IPsec supports HMAC_DRBG with HMAC-SHA2-256 which uses SHA2-256. IPsec uses the HP FutureSmart Firmware Linux Kernel Crypto API for these algorithms. For more details on the HMAC algorithms, see the TSS for FCS_COP.1(g).<br><br>*Trusted update*<br><br>The TOE's trusted update function uses the SHA2-256 algorithm for RSA digital signature verification. This function uses the HP FutureSmart Firmware OpenSSL 1.1.1 implementation of the SHA2-256 algorithm. For more details on trusted update, see the TSS for FPT_TUD_EXT.1.<br><br>*TSF testing*<br><br>The TOE's TSF testing (Whitelisting) function uses the SHA2-256 algorithm for RSA digital signature verification. This function uses the HP FutureSmart Firmware OpenSSL 1.1.1 implementation of the SHA2-256 algorithm. For more details on TSF testing, see the TSS for FPT_TST_EXT.1.<br><br>*Storage encryption*<br><br>For the Customer Data Encryption feature, the volume key is used to encrypt the customer data partition and is protected using a passphrase. A key is derived by performing PBKDF2 function using the passphrase as input. The derived key is the key that is used to encrypt/decrypt the volume key. |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|

One of the primitives of PBKDF2 is the SHA2-256 algorithm. This function uses the HP FutureSmart Firmware OpenSSL 1.1.1 implementation of the SHA2-256 algorithm.

In addition, the TSF uses the SHA2-256 algorithm in HP FutureSmart Firmware OpenSSL 1.1.1 when combining the intermediate key (along with static data) used to generate the data encryption key for encrypting/decrypting the JDI configuration file used to store IPsec pre-shared keys.

For additional information on storage encryption, see FDP_DSK_EXT.1.

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

**Table 49: SHS algorithms**

| Usage | Implementation | Purpose | Algorithm |
|---|---|---|---|
| IKE | HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module | Pre-shared keys | SHA-1, SHA2-256, SHA2-512 |
| | | KAS FFC | SHA2-256 |
| | | RSA digital signature generation | SHA2-256, SHA2-384, SHA2-512 |
| | | RSA digital signature verification | SHA-1, SHA2-256, SHA2-384, SHA2-512 |
| | | HMAC | SHA2-256, SHA2-384, SHA2-512 |
| IPsec | HP FutureSmart Firmware Linux Kernel Crypto API | HMAC | SHA-1, SHA2-256, SHA2-384, SHA2-512 |
| | | HMAC (HMAC_DRBG) | SHA2-256 |
| Trusted update | HP FutureSmart Firmware OpenSSL 1.1.1 | RSA digital signature verification | SHA2-256 |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|

| | | | |
|---|---|---|---|
| TSF testing | HP FutureSmart Firmware OpenSSL 1.1.1 | RSA digital signature verification | SHA2-256 |
| Storage encryption | HP FutureSmart Firmware OpenSSL 1.1.1 | PBKDF2 | SHA2-256 |
| | | Submask combining | SHA2-256 |

| | |
|---|---|
| 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.* |
| Resp | IKE 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.<br><br>IKE supports SHA2-256 for KAS FFC as specified in TSS for FCS_CKM.1(a). For more details on KAS FFC, see the TSS for FCS_CKM.1(a).<br><br>IKE 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).<br><br>IKE also supports HMAC algorithms using SHA2-256, SHA2-384, and SHA2-512. For more details on the HMAC algorithms, see the TSS for FCS_COP.1(g).<br><br>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. For more details on the HMAC algorithms, see the TSS for FCS_COP.1(g).<br><br>IPsec supports HMAC_DRBG with HMAC-SHA2-256 which uses SHA2-256. For more details on the HMAC algorithms, see the TSS for FCS_COP.1(g).<br><br>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.<br><br>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. |

| | |
|---|---|
| FCS_COP.1(d) (AES) | **Objective(s)**:<br>• O.STORAGE_ENCRYPTION<br><br>**Summary**: |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an eMMC. The TSF ensures that User Document Data and confidential TSF Data is not stored as plaintext on the eMMC drive.<br><br>The following User Document Data and confidential TSF data are stored on the eMMC:<br>• User Document Data:<br>  ○ Stored jobs (copy/print/fax)<br>  ○ Temporary job files<br>• Confidential TSF data:<br>  ○ Private keys corresponding to identity certificates<br>  ○ IPsec pre-shared keys<br>All User Document Data and confidential TSF data are encrypted using AES in CBC mode with a 256 bit key. For additional details, see FDP_DSK_EXT.1.</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.</td></tr>
<tr><td></td><td>Resp</td><td>The Summary section above provides a description of the key size and mode used for encryption.</td></tr>
<tr><td>FCS_COP.1(f) (Key Encryption)</td><td colspan="2"><u>Objective(s)</u>:<br>• O.STORAGE_ENCRYPTION<br><br><u>Summary</u>:<br><br>The TSF implements a feature called Customer Data Encryption. The Customer Data Encryption feature encrypts data (which includes User Document Data) stored on the partition designated for storing customer data on the eMMC drive.<br><br>The volume key is used to encrypt the customer data partition and is protected using a passphrase. A key is derived by performing PBKDF2 using the passphrase as input. The derived key is used to encrypt/decrypt the volume key.<br><br>The volume key is encrypted/decrypted using the AES-CBC-256 algorithm in the HP FutureSmart Firmware Linux Kernel Crypto API.<br><br>For additional details on the keys used for Customer Data Encryption, see the [KMD].</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall verify the TSS includes a description of the key encryption function(s) and shall verify the key encryption uses an approved algorithm according to the appropriate specification.</td></tr>
<tr><td></td><td>Resp</td><td>The Summary section above provides a description of the key encryption function.</td></tr>
<tr><td>FCS_COP.1(g) (HMAC)</td><td colspan="2"><u>Objective(s)</u>: O.COMMS_PROTECTION<br><br><u>Summary</u>:<br><br><u>IKE</u></td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
IKE supports the keyed-hash message authentication algorithms and key sizes specified in Table 50 using the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module meeting [FIPS180-4] (which supersedes FIPS 180-3 specified in the SFR) and [FIPS198-1].<br><br>
IKE uses truncated HMACs. Table 50 also shows the actual digest sizes and the truncated digest sizes. For more details on the required HMAC algorithms, see the TSS for FCS_IPSEC_EXT.1.<br><br>
<u>IPsec</u><br><br>
IPsec support the keyed-hash message authentication algorithms and key sizes specified in Table 50 using the HP FutureSmart Firmware Linux Kernel Crypto API meeting [FIPS180-4] (which supersedes FIPS 180-3 specified in the SFR) and [FIPS198-1].<br><br>
IPsec use truncated HMACs. Table 50 also shows the actual digest sizes and the truncated digest sizes. For more details on the required HMAC algorithms, see the TSS for FCS_IPSEC_EXT.1.<br><br>
IPsec supports HMAC_DRBG with HMAC-SHA2-256 which uses SHA2-256.<br><br>
Table 50: HMAC algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Algorithm</th><th>Key size</th><th>Actual/Trunc. Digest size</th></tr>
<tr><td rowspan="4">IKE</td><td rowspan="4">HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module</td><td>HMAC-SHA1-96</td><td>160 bits</td><td>160/96 bits</td></tr>
<tr><td>HMAC-SHA2-256-128</td><td>256 bits</td><td>256/128 bits</td></tr>
<tr><td>HMAC-SHA2-384-192</td><td>384 bits</td><td>384/192 bits</td></tr>
<tr><td>HMAC-SHA2-512-256</td><td>512 bits</td><td>512/256 bits</td></tr>
<tr><td rowspan="4">IPsec</td><td rowspan="4">HP FutureSmart Firmware Linux Kernel Crypto API</td><td>HMAC-SHA1-96</td><td>160 bits</td><td>160/96 bits</td></tr>
<tr><td>HMAC-SHA2-256-128</td><td>256 bits</td><td>256/128 bits</td></tr>
<tr><td>HMAC-SHA2-384-192</td><td>384 bits</td><td>384/192 bits</td></tr>
<tr><td>HMAC-SHA2-512-256</td><td>512 bits</td><td>512/256 bits</td></tr>
</table>
<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(h) (HMAC)</td><td><u>Objective(s)</u>:<br>• 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"><u>Summary</u>:<br><br>As discussed in FDP_DSK_EXT.1, the TSF implements a feature called Customer Data Encryption. The Customer Data Encryption feature encrypts data (including User Document Data) stored on the partition designated for storing customer data on the eMMC drive.<br><br>The volume key is used to encrypt the customer data partition and is protected using a passphrase. A key is derived by performing PBKDF2 using the passphrase as input. The derived key is the key that is used to encrypt/decrypt the volume key.<br><br>One of the primitives of PBKDF2 is HMAC-SHA-256. The key length of the HMAC-SHA-256 algorithm is 256 bits. The block size is 512 bits. The output MAC length used is 256 bits.<br><br>For additional details on the keys used for Customer Data Encryption, see the [KMD].</td></tr>
<tr><td></td><td>AA</td><td>The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.</td></tr>
<tr><td></td><td>Resp</td><td>The Summary section above provides a description of the HMAC function used as a primitive of PBKDF2.</td></tr>
<tr><td>FCS_IPSEC_EXT.1 (IPsec)</td><td colspan="2"><u>Objective(s)</u>: O.COMMS_PROTECTION<br><br><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.<br><br>IPsec supports both PSKs and X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), and Internet Key Exchange version 1 (IKEv1) protocol.<br><br>IKEv1 supports following cryptographic algorithms.<br>• DH (dhEphem) P=2048, SHA2-256 (FCS_CKM.1(a))<br>• DSA (FCS_CKM.1(a))<br>  ○ L=2048, N=224<br>  ○ L=2048, N=256<br>  ○ L=3072, N=256<br>• RSA 2048-bit and 3072-bit signature generation/verification (FCS_COP.1(b))<br>• AES-CBC-128, AES-CBC-256, and AES-ECB-256 (FCS_COP.1(a))<br>• HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1(g))<br>• CTR_DRBG(AES) (FCS_RBG_EXT.1)<br><br>IPsec ESP supports the following cryptographic algorithms.<br>• AES-CBC-128 and AES-CBC-256 (FCS_COP.1(a))</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | • HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1(g))<br>• HMAC_DRBG (FCS_RBG_EXT.1)<br><br>The TOE imports the RSA keys—in the form of X.509v3 certificates—used by IKEv1 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 for peer authentication. For more information on the TOE's certificate management capabilities, see the TSS for FMT_MTD.1 for certificate importing.<br><br>IKEv1 supports DH/DSA in phase 1 to establish a protected connection using KAS FFC, respectively. Random values generated for KAS FFC 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.<br><br>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.)<br><br>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.<br><br>The TOE's IKEv1 supports the following DH Groups. The DH groups are specified using a defined group description as specified in [RFC3526].<br>• DH Group 14 (2048-bit MODP)<br>• DH Group 15 (3072-bit MODP)<br>• DH Group 16 (4096-bit MODP)<br>• DH Group 17 (6144-bit MODP)<br>• DH Group 18 (8192-bit MODP)<br><br>All TOE cryptographic functions used by IKE are implemented in the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module.<br><br>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.<br><br>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.<br><br>The TOE's IPsec is conformant to the MUST/MUST NOT requirements of the following Internet Engineering Task Force (IETF) Request for Comments (RFCs).<br>• [RFC3602] for use of AES-CBC-128 and AES-CBC-256 in IPsec<br>• [RFC4301] for IPsec |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | • [RFC4303] for ESP<br>• [RFC4304] for extended sequence numbers<br>• [RFC2407] and [RFC2408] for ISAKMP<br>• [RFC2409] and [RFC4109] for IKEv1<br>• [RFC4868] for SHA-2 HMAC in IPsec<br><br>*Incoming packet processing*<br><br>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.<br><br>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 IPsec rules are applied. The 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 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.<br><br>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 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.<br><br>*Outgoing packet processing*<br><br>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.<br><br>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* |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | | *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.*<br><br>*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:<br>• AES-CBC-128 and AES-CBC-256 (FCS_COP.1(a))<br>• HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1(g)) |
| | 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. |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | 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_KDF_EXT.1 (Key Derivation) | **Objective(s)**:<br>• O.STORAGE_ENCRYPTION<br><br>**Summary**:<br>As discussed in FDP_DSK_EXT.1, the TSF implements a feature called Customer Data Encryption. The Customer Data Encryption feature encrypts data (including User Document Data) stored on the partition designated for storing customer data on the eMMC drive.<br><br>The volume key is used to encrypt the customer data partition and is protected using a passphrase. A key is derived by performing PBKDF2 using the passphrase as input. The derived key is the key that is used to encrypt/decrypt the volume key.<br><br>The PBKDF2 implementation in HP FutureSmart Firmware OpenSSL 1.1.1 is used to derive the key that is used to encrypt/decrypt the volume key. The PBKDF2 implementation in HP FutureSmart Firmware OpenSSL 1.1.1 is defined in NIST SP 800-132.<br><br>For additional details on the keys used for Customer Data Encryption, see the [KMD]. | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | AA | *The evaluator shall verify the TSS includes a description of the key derivation function and shall verify the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-108 and SP800-132.* |
| | Resp | Response is contained in Summary above. |
| FCS_KYC_EXT.1/CDE (Key chaining) | **Objective(s)**: O.STORAGE_ENCRYPTION<br><br>**Summary**: The TSF implements a feature called Customer Data Encryption that encrypts data stored on the partition designated for storing customer data on the eMMC drive. In the evaluated configuration, the Customer Data Encryption feature is configured to encrypt data using AES-CBC-256.<br><br>The keychain for the Customer Data Encryption feature is comprised of the following keys: passphrase, derived key (key encryption key), and volume key.<br><br>When the HCD is powered on for the first time, the TSF generates a 256-bit passphrase and a 256-bit volume key using the CTR_DRBG(AES) algorithm in HP FutureSmart Firmware OpenSSL 1.1.1. The TSF derives (as specified in FCS_KDF_EXT.1) a 256-bit key encryption key from the 256-bit passphrase. The TSF encrypts (as specified in FCS_COP.1(f)) the 256-bit volume key using the 256-bit key encryption key and stores the encrypted 256-bit volume key on the eMMC drive. The TSF stores the 256-bit passphrase in plaintext in NVRAM.<br><br>On each subsequent HCD boot, the TSF reads the 256-bit passphrase stored in NVRAM and derives (as specified in FCS_KDF_EXT.1) the 256-bit key encryption key from the 256-bit passphrase. The TSF reads the encrypted 256-bit volume key stored on the eMMC drive and decrypts (as specified in FCS_COP.1(f)) the encrypted 256-bit volume key using the 256-bit key encryption key.<br><br>The TSF uses the 256-bit volume key to encrypt/decrypt data stored on the customer data partition on the eMMC drive.<br><br>In the evaluated configuration, the key chain supports a volume key output of no fewer than 256 bits.<br><br>For additional information on the key chain used for Customer Data Encryption, see [KMD]. | |
| | AA | *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.* |
| | Resp | See Summary above for description. |
| FCS_KYC_EXT.1/CM (Key chaining) | **Objective(s)**: O.STORAGE_ENCRYPTION<br><br>**Summary**: The TSF stores the network identity certificate and its corresponding private key in encrypted form in a certificates XML file stored on the eMMC drive. AES-CBC-256 is used to encrypt the network identity certificate and its private key contained in the certificates XML file.<br><br>The keychain for certificates XML file encryption is comprised of the following keys: data encryption key. | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | When the HCD is powered on for the first time, the TSF generates a 256-bit data encryption key using the CTR_DRBG(AES) algorithm in HP FutureSmart Firmware OpenSSL 1.1.1. The TSF stores the 256-bit data encryption key in plaintext in NVRAM.<br>On each subsequent HCD boot, the TSF reads the 256-bit data encryption key from NVRAM.<br>The TSF uses the 256-bit data encryption key to encrypt/decrypt (as specified in FCS_COP.1(d)) the certificates XML file stored on the eMMC drive.<br>The key chain supports a data encryption key output of no fewer than 256 bits.<br>For additional information on the key chain used for Certificate Data Encryption, see [KMD]. | |
| | AA | *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.* |
| | Resp | See Summary above for description. |
| FCS_KYC_EXT.1/CMT (Key chaining) | **Objective(s)**: O.STORAGE_ENCRYPTION<br>**Summary**: The TSF stores identity certificates and their corresponding private keys in individual files (a.k.a., thumbprint files) stored in encrypted form on the eMMC drive. AES-CBC-256 is used to encrypt thumbprint files.<br>The keychain for thumbprint file encryption is comprised of the following keys: intermediate key and data encryption key.<br>When the HCD is powered on for the first time, the TSF generates a 256-bit intermediate key using the CTR_DRBG(AES) algorithm in HP FutureSmart Firmware OpenSSL 1.1.1. The TSF stores the 256-bit intermediate key in plaintext in NVRAM. The TSF combines (as specified in FCS_SMC_EXT.1/CMT) the 256-bit intermediate key and a 256-bit submask value to generate the 256-bit data encryption key.<br>On each subsequent HCD boot, the TSF reads the 256-bit intermediate key stored in NVRAM. The TSF combines (as specified in FCS_SMC_EXT.1/CMT) the 256-bit intermediate key and a 256-bit submask value to generate the 256-bit data encryption key.<br>The TSF uses the 256-bit data encryption key to encrypt/decrypt (as specified in FCS_COP.1(d)) thumbprint files stored on the eMMC drive.<br>The key chain supports a data encryption key output of no fewer than 256 bits.<br>For additional information on the key chain used for Certificate Data Encryption, see [KMD]. | |
| | AA | *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.* |
| | Resp | See Summary above for description. |
| | **Objective(s)**: O.STORAGE_ENCRYPTION | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| FCS_KYC_EXT.1/JCF (Key chaining) | **Summary**: The TSF encrypts the JDI configuration file containing IPsec pre-shared keys and other networking configuration data. The JDI configuration file is stored on the eMMC drive and is encrypted using AES-CBC-256.<br><br>The keychain for JDI configuration file encryption is comprised of the following keys: intermediate key and data encryption key.<br><br>When the HCD is powered on for the first time, the TSF generates a 256-bit intermediate key using the CTR_DRBG(AES) algorithm in HP FutureSmart OpenSSL 1.1.1. The TSF stores the 256-bit intermediate key in plaintext in NVRAM. The TSF combines (as specified in FCS_SMC_EXT.1/JCF) the 256-intermediate key, HCD's serial number, and HCD's MAC address to generate a 256-bit data encryption key.<br><br>On each subsequent HCD boot, the TSF reads the 256-bit intermediate key stored in NVRAM. The TSF combines (as specified in FCS_SMC_EXT.1/JCF) the 256-intermediate key, HCD's serial number, and HCD's MAC address to generate a 256-bit data encryption key.<br><br>The TSF encrypts/decrypts (as specified in FCS_COP.1(d)) the JDI configuration file using the 256-bit data encryption key.<br><br>The key chain supports a data encryption key output of no fewer than 256 bits.<br><br>For additional information on the key chain used for JDI configuration file encryption, see [KMD]. | |
| | AA | *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.* |
| | Resp | See Summary above for description. |
| FCS_RBG_EXT.1 (DRBG) | **Objective(s)**: O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION<br><br>**Summary**: IKE uses the CTR_DRBG(AES) DRBG algorithm from the HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module 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) is used by this DRBG.<br><br>IPsec uses the HMAC_DRBG algorithm with HMAC-SHA2-256 in the HP FutureSmart Firmware Linux Kernel Crypto API. The HMAC-SHA2-256 algorithm claimed in FCS_COP.1(g) is used by this DRBG.<br><br>The storage encryption function includes encryption/decryption of customer data, private keys associated with identity certificates, and the pre-shared key stored on the eMMC. The TSF uses the CTR_DRBG(AES) algorithm from HP FutureSmart Firmware OpenSSL 1.1.1 to generate keys to use in the process of encrypting the above data. This DRBG supports the AES 256-bit algorithm. The AES-CTR-256 algorithm claimed in FCS_COP.1(d) is used by this DRBG.<br><br>The three DRBGs are seeded by a hardware-based entropy noise source. This entropy source provides at least 256 bits of minimum entropy. | |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">
Table 51: DRBG algorithms
<table>
<tr><th>Usage</th><th>Implementation</th><th>Modes and key sizes</th></tr>
<tr><td>IKE</td><td>HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module</td><td>CTR_DRBG(AES)</td></tr>
<tr><td>IPsec</td><td>HP FutureSmart Firmware Linux Kernel Crypto API</td><td>HMAC_DRBG(HMAC-SHA2-256)</td></tr>
<tr><td>Storage encryption</td><td>HP FutureSmart Firmware OpenSSL 1.1.1</td><td>CTR_DRBG(AES)</td></tr>
</table>
</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>
<tr><td></td><td>Resp</td><td>The TOE implements three DRBGs. One is used by IKE, another is used by IPsec, and another is used for storage encryption.</td></tr>
<tr><td>FCS_SMC_EXT.1/JCF (Submask Combining)</td><td colspan="2"><u>Objective(s)</u>: O.STORAGE_ENCRYPTION<br><br><u>Summary</u>: The TSF uses the SHA2-256 algorithm in HP FutureSmart Firmware OpenSSL 1.1.1 and the exclusive OR (XOR) operation to combine the 256-bit intermediate key and other submask values to generate the 256-bit data encryption key for encrypting/decrypting the JDI configuration file.<br><br>For additional details on the process used to generate the encryption key for encrypting/ decrypting the JDI configuration file, see [KMD].</td></tr>
<tr><td></td><td>AA</td><td>If keys are XORed together to form an intermediate key, the TSS section shall identify how this is performed (e.g., if there are ordering requirements, checks performed, etc.). The evaluator shall also confirm that the TSS describes how the length of the output produced is at least the same as that of the DEK.</td></tr>
<tr><td></td><td>Resp</td><td>See Summary above.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td>FCS_SMC_EXT.1/CMT (Submask Combining)</td><td colspan="2"><u>Objective(s)</u>: O.STORAGE_ENCRYPTION<br><br><u>Summary</u>: The TSF stores the identity certificates and their corresponding private keys in encrypted individual files (a.k.a., thumbprint files) on the eMMC drive.<br><br>The TSF performs an exclusive OR (XOR) operation to combine a 256-bit intermediate key and a 256-bit submask value to generate the 256-bit data encryption key. The data encryption key is used by the TSF to encrypt/decrypt the thumbprint files.<br><br>For additional details on the process used to generate the data encryption key for encrypting/ decrypting thumbprint files, see [KMD].</td></tr>
<tr><td></td><td>AA</td><td>If keys are XORed together to form an intermediate key, the TSS section shall identify how this is performed (e.g., if there are ordering requirements, checks performed, etc.). The evaluator shall also confirm that the TSS describes how the length of the output produced is at least the same as that of the DEK.</td></tr>
<tr><td></td><td>Resp</td><td>See Summary above.</td></tr>
<tr><td>FDP_ACC.1 (Subset access control)</td><td colspan="2"><u>Objective(s)</u>: O.ACCESS_CONTROL, O.USER_AUTHORIZATION<br><br><u>Summary</u>: [HCDPP] predefines the subjects, objects, and operations. Table 30 and Table 31 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"><u>Objective(s)</u>: O.ACCESS_CONTROL, O.USER_AUTHORIZATION<br><br><u>Summary</u>: In this section, Table 30 is explained first followed by Table 31.<br><br><u>Print Create D.USER.DOC in Table 28</u><br><br>Print jobs are submitted to the TOE over the network using PJL. Any computer that can connect to the TOE using IPsec can submit a print job. The TOE requires a user identity (a.k.a. job owner) to be included with each print job, but this user identity is unauthenticated. For this reason, the job owner, U.ADMIN, and U.NORMAL boxes in Table 30 for "Print Create" are marked as not applicable (n/a) because the job owner is always unauthenticated. If no job owner is provided with the print job, the print job is rejected by the TOE.<br><br>Required security attributes:<br>• Subject: None (Unauthenticated user)<br>• Object: Job owner<br><br><u>Print Read/Modify/Delete D.USER.DOC in Table 30</u><br><br>In order to print, the user must log in via the Control Panel. Each print job, when created, must have a user identity supplied by the client computer. This user identity is used as the job owner. The logged in user's identity must match the user identity of the print job in order for the logged in user to be considered the job owner. Only the job owner can print (read) the job. Only the job</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | owner and U.ADMIN can delete a print job. By design, the D.USER.DOC information of a print job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Scan Create/Read/Modify/Delete D.USER.DOC in Table 30*<br><br>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. The U.ADMIN can delete a scan job. By design, the D.USER.DOC information of a scan job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Copy Create/Read/Modify/Delete D.USER.DOC in Table 30*<br><br>In order to copy a document, the user must be logged into the TOE via the Control Panel. During the copy process, the job is owned by the user who initiated it. The job owner can create, read, and delete a copy job. The U.ADMIN can delete a copy job. By design, the D.USER.DOC information of a copy job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Fax send Create/Read/Modify/Delete D.USER.DOC in Table 30*<br><br>In order to perform a fax send job, the user must be logged into the TOE via the Control Panel. During the fax sending process, the job is owned by the user who initiated it. The job owner can create, read, and delete a fax send job. The U.ADMIN can delete a fax send job. By design, the D.USER.DOC information of a fax send job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Fax receive Create/Read/Modify/Delete D.USER.DOC in Table 30*<br><br>All incoming faxes are owned by the Device Administrator account. In order to access a fax receive job, the fax owner or another U.ADMIN must be logged into the TOE via the Control Panel. The fax owner (i.e., Device Administrator) can create a fax receive job. Both the fax owner and another U.ADMIN can read and delete a fax receive job. By design, the D.USER.DOC information of a fax receive job cannot be modified by anyone.<br><br>Required security attributes: |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | • Subject: Control Panel user identity/role<br>• Object: Fax owner<br><br>*Storage / retrieval Create/Read/Modify/Delete D.USER.DOC in Table 30*<br><br>Print jobs and fax received jobs can be stored in Job Storage.<br><br>For print jobs, client computers connect over IPsec to submit print jobs via PJL. The users of these client computers can submit print jobs which are then stored in Job Storage by the TOE. The TOE requires each print job to contain a user identity that is then used as the job owner of the print job. This user identity is unauthenticated and can be any identity the submitter on the client computer chooses. Thus, for print jobs, only unauthenticated users can store a print job in Job Storage. This is why "allowed" is shown for "create" in Table 30 for unauthenticated users. Only the job owner can "read" a print job from Job Storage. Both the job owner and any administrator can delete a print job from Job Storage. By design, the D.USER.DOC information of a print job in Job Storage cannot be modified by anyone.<br><br>Fax receive jobs are stored in Job Storage. All incoming faxes are owned by the Device Administrator account. In order to access a fax receive job in Job Storage, the job owner or another U.ADMIN must be logged into the TOE via the Control Panel. Only the job owner (i.e., Device Administrator) can create a fax receive job. Both the job owner and another U.ADMIN can read and delete a fax receive job. By design, the D.USER.DOC information of a fax receive job in Job Storage cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Unauthenticated users (create print job only) or Control Panel user identity/role<br>• Object: Job owner<br><br>*Print Create/Read/Modify/Delete D.USER.JOB in Table 31*<br><br>For the same reasons described in "Print Create D.USER.DOC" above, the job owner, U.ADMIN, and U.NORMAL, are marked as not applicable (n/a) because the job owner is always unauthenticated.<br><br>Job owner, U.ADMIN, and U.NORMAL can view the print queue, thus, they can see all print jobs, but only the job owner and U.ADMIN can view the print log. Unauthenticated users cannot view the print queue or print log.<br><br>Only the job owner and U.ADMIN can delete the print job of a job owned by the job owner.<br><br>By design, the D.USER.JOB information of a print job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Unauthenticated user (create print job and view print queue only) or Control Panel user identity/role<br>• Object: Job owner<br><br>*Scan Create/Read/Modify/Delete(Cancel) D.USER.JOB in Table 31* |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | 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. Other U.NORMAL users can view the scan status, but not the scan log. By design, the D.USER.JOB information of a scan job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Copy Create/Read/Modify/Delete D.USER.JOB in Table 31*<br><br>In order to copy a document, the user must be logged into the TOE via the Control Panel. When the job is copied (i.e., created), the job is owned by the logged in user. Neither an administrator nor another user can create a copy job under a different user identity. The job owner can create, view the copy status/log, and cancel a copy job owned by the job owner. An administrator (U.ADMIN) can view the copy status/log, and cancel a copy job. Other U.NORMAL users can view the copy status, but not the copy log. By design, the D.USER.JOB information of a copy job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Fax send Create/Read/Modify/Delete D.USER.JOB in Table 31*<br><br>In order to perform a fax send job, the user must be logged into the TOE via the Control Panel. During the fax sending process, the job is owned by the user who initiated it. The job owner can create, view the fax send queue/log, and cancel a fax send job owned by the job owner. An administrator (U.ADMIN) can view the fax send status/log, and cancel a fax send job. Other U.NORMAL and users can view the fax send status, but not the fax send log. By design, the D.USER.JOB information of a fax send job cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Job owner<br><br>*Fax receive Create/Read/Modify/Delete D.USER.JOB in Table 31*<br><br>All incoming faxes are owned (i.e., created) by the Device Administrator account. In order to access a fax receive job, the fax owner, or another U.ADMIN must be logged into the TOE via the Control Panel. Both the fax owner and another U.ADMIN can view the fax receive status/log, and delete a fax receive job owned by the job owner. Other U.NORMAL users can view the fax receive status, but not the fax receive log. By design, the D.USER.JOB information of a fax receive job cannot be modified by anyone. |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">Required security attributes:<br>• Subject: Control Panel user identity/role<br>• Object: Fax owner<br><br><u>Storage / retrieval Create/Read/Modify/Delete D.USER.JOB in Table 31</u><br><br>Print jobs and fax received jobs can be stored in Job Storage.<br><br>For print jobs, client computers connect over IPsec to submit print jobs via PJL. The users of these client computers can submit print jobs which are stored in Job Storage. The TOE requires each print job to contain a user identity that is then used as the job owner of the print job. This user identity is unauthenticated and can be any identity the submitter on the client computer chooses. Thus, for print jobs, only unauthenticated users can store a print job in Job Storage. This is why "allowed" is shown for "create" in Table 31 for unauthenticated users. The job owner and U.ADMIN can view the list of jobs in Job Storage owned by the job owner. By design, the U.USER.JOB information of a print job stored in Job Storage cannot be modified.<br><br>Fax receive jobs are stored in Job Storage. All incoming faxes are owned by the Device Administrator account. In order to access a fax receive job, the job owner, or another U.ADMIN must be logged into the TOE via the Control Panel. Only the job owner (i.e., Device Administrator) can create a fax receive job. Both the job owner and another U.ADMIN can read and delete a fax receive job. The fax receive job's D.USER.JOB cannot be modified by anyone.<br><br>Required security attributes:<br>• Subject: Unauthenticated users (create print job only) or Control Panel user identity/role<br>• 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 30 and Table 31.</td></tr>
<tr><td></td><td>Resp</td><td>See the description above.</td></tr>
<tr><td>FDP_DSK_EXT.1<br>(Disk data protection)</td><td colspan="2"><u>Objective(s)</u>: O.STORAGE_ENCRYPTION<br><br><u>Summary</u>: The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an eMMC.<br><br>[HCDPP] states that SEDs must be CC certified using the Full Disk Encryption (FDE) Encryption Engine (EE) collaborative PP (cPP) or perform encryption in accordance with FCS_COP.1(d). The TOE performs encryption of User Document Data and confidential TSF data according to FCS_COP.1(d) without any user intervention.<br><br>The encryption and decryption implementation is built into the TOE firmware.<br><br><u>Customer Data Encryption</u><br><br>The TSF implements a feature called Customer Data Encryption that is based on the device-mapper crypt (dm-crypt) target. dm-crypt provides transparent encryption of block devices using the Linux Kernel Crypto API. The Customer Data Encryption feature encrypts customer data</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | (including User Document Data) stored on the partition on the eMMC designated for storing customer data. In the evaluated configuration, data stored on the customer data partition is encrypted using the AES-CBC-256 implementation in the Linux Kernel Crypto API.<br><br>Data stored on the encrypted partition includes: Stored jobs (e.g., print, copy, fax), temporary job files, PJL and PostScript filesystem files including downloaded fonts, and extensibility customer data (if stored there by the extensibility solution).<br><br>A volume key is used to encrypt the customer data partition. The volume key is generated using the CTR_DRBG in HP FutureSmart Firmware OpenSSL 1.1.1 when the HCD is powered on for the first time.<br><br>The volume key is protected using a passphrase. As with the volume key, the passphrase is generated using a CTR_DRBG when the HCD is powered on for the first time. A key is derived by performing PBKDF2 using the passphrase as input. The derived key is the key that is used to encrypt/decrypt the volume key.<br><br>For additional details on the passphrase, derived key, or volume key, see the [KMD].<br><br>*Certificate Data Encryption*<br><br>The TSF encrypts identity certificates and their corresponding private keys on the eMMC.<br><br>When an identity certificate with private key is imported, the TSF stores the certificate along with the private key in encrypted form. The certificate with private key is encrypted using the AES-CBC-256 implementation in HP FutureSmart Firmware OpenSSL 1.1.1.<br><br>The key used to encrypt certificate data is generated using the CTR_DRBG in HP FutureSmart Firmware OpenSSL 1.1.1 when the HCD is powered on for the first time.<br><br>For additional details on the key used to encrypt certificate data, see the [KMD].<br><br>*JDI Configuration File Encryption*<br><br>The TSF encrypts the JDI configuration file which contains the IPsec pre-shared keys and other network configuration information. The JDI configuration file is stored the eMMC outside of the customer data partition.<br><br>When an IPsec pre-shared key is created or updated, the TSF writes this pre-shared key to the JDI configuration file and encrypts the file using the AES-CBC-256 implementation in HP FutureSmart Firmware OpenSSL 1.1.1.<br><br>On every HCD boot, the TSF generates the data encryption key used to encrypt the JDI configuration file by combining an intermediate key and static data (e.g., MAC address, etc.).<br><br>The intermediate key is generated using the CTR_DRBG in HP FutureSmart Firmware OpenSSL 1.1.1 when the HCD is powered on for the first time.<br><br>For additional details on the key used to encrypt the JDI configuration file, see the [KMD]. | |
| | AA | *As per NIAP Technical Decision [CCEVS-TD0176]* |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | | *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.*<br><br>*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.*<br><br>*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.*<br><br>*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.* |
| | Resp | The Summary section above provides the necessary description for this assurance activity. |
| FDP_FXS_EXT.1 (Fax separation) | **Objective(s)**: O.FAX_NET_SEPARATION<br><br>**Summary**:<br><br>*Fax separation*<br><br>The TOE provides the separation of fax from the Ethernet. The fax functionality is limited to transmitting and receiving user data using fax protocols. The architecture and design provide separation between the analog fax processing board and the network controller. System components that control the analog fax hardware have no functions to access the network hardware. Faxes from a phone line cannot be sent into the network or influence other resources on the network.<br><br>The analog fax functions of the TOE support the sending and receiving of fax data. The closed nature of analog fax firmware with its limited functionality does not provide a pathway or support for commands necessary to achieve network access.<br><br>Sending and receiving of data through the serial fax modem can only occur during an active fax session. A fax session can only be established between two fax modems that successfully negotiate common capabilities such as fax resolution, transmission speed, compression, and format. Fax negotiation and communication uses the T.30 protocol, which is restricted to fax communications. A fax session cannot be negotiated for anything other than a fax transfer, so it is not possible for other components in or out of the system to use the modem for transferring data other than fax data. | |

<table>
<tr><th>TOE SFRs</th><th>TOE SFR compliance rationale</th></tr>
<tr><td></td><td>
The analog fax hardware and the firmware that controls the fax hardware do not have the ability to access the Ethernet fax functions. No pathway is provided to the Ethernet interface from the fax. The TOE's analog fax functions only support the sending and receiving of fax data. Fax commands with potential for accessing the Ethernet are not supported by the TOE.<br><br>
<u>Fax use cases</u><br><br>
The TOE supports the following fax use cases in the evaluated configuration.<br>
• Fax send<br>
• Fax receive<br>
• Storing of received faxes<br><br>
<u>Fax capabilities</u><br><br>
Table 52: Telecommunications acronyms
<table>
<tr><th>Acronym</th><th>Definition</th></tr>
<tr><td>CCITT</td><td>Consultative Committee for International Telephony and Telegraphy</td></tr>
<tr><td>EIA</td><td>Electronic Industries Alliance</td></tr>
<tr><td>ITU-T</td><td>International Telegraph Union Telecommunication Standardization Sector</td></tr>
<tr><td>TIA</td><td>Telecommunications Industry Association</td></tr>
</table>
The TOE supports the following fax protocols in the evaluated configuration.<br>
• CCITT/ITU-T Group 3<br>
• CCITT/ITU-T T.30<br>
• TIA/EIA Class 1<br>
• TIA/EIA Class 2<br>
• TIA/EIA Class 2.0<br>
• TIA/EIA Class 2.1<br><br>
The TOE supports the following fax compression methods in the evaluated configuration.<br>
• Joint Bi-level Image Experts Group (JBIG)<br>
• Modified Huffman (MH)<br>
• Modified READ (MR)<br>
• Modified Modified READ (MMR)<br><br>
The TOE supports the following fax transmission standards and speeds in the evaluated configuration with a modem speed of up to 33.6 kilobits per second (kbps).<br>
• V.17 at 14,400, 12,000, 9,600, 7,200 bps<br>
• V.33 at 14,400, 12,000 bps
</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | • V.29 at 9,600, 7,200 bps<br>• V.27 at 4,800, 2,400 bps<br>• V.34 at 33,600, 31,200, 28,800, 26,400, 24,000, 21,600, 19,200, 16,800 bps<br><br>The TOE supports the following fax resolutions in the evaluated configuration.<br>• Standard - 200 x 100 dots per inch (dpi)<br>• Fine - 200 x 200 dpi<br>• Superfine - 300 x 300 dpi<br>• Ultrafine - 200 x 400 (receive only)<br>• Ultrafine - 400 x 400 (receive only) | |
| | AA | *The evaluator shall check the TSS to ensure that it describes:*<br>*1) The fax interface use cases*<br>*2) The capabilities of the fax modem and the supported fax protocols*<br>*3) The data that is allowed to be sent or received via the fax interface*<br>4) *How the TOE can only be used transmitting or receiving User Data using fax protocols* |
| | Resp | These descriptions are provided above. |
| FIA_AFL.1 (Authentication failure handling) | **Objective(s)**: O.USER_I&A<br><br>**Summary**: This SFR applies to the Local Device Sign In mechanism (used by the Control Panel, EWS, and REST interfaces). The only account associated with this mechanism is the Device Administrator account.<br><br>The lockout mechanism uses the following control values.<br>• Account lockout maximum attempts<br>• Account lockout interval<br>• Account reset lockout counter interval<br><br>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 reset 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.<br><br>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.<br><br>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 | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | attempts counter is reset to zero. This value must be equal to or greater than the account lockout interval value. | |
| | AA | *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.* |
| | Resp | 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.<br>Caveats are:<br>• Consecutive failed authentication attempts using the same authentication credential count as a single failed authentication attempt.<br>• 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. |
| FIA_ATD.1 (User attribute definition) | **Objective(s)**: O.USER_AUTHORIZATION<br>**Summary**:<br>*Control Panel users*<br>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.<br>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.<br>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.<br>*EWS users*<br>The EWS authentication works very similarly to the Control Panel authentication.<br>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 | |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">Password. The Device Administrator Password's composition requirements are defined in FIA_PMG_EXT.1.<br><br>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.<br><br><u>REST users</u><br><br>For the REST interface, this interface is an administrator-only interface used to manage the TOE over IPsec.<br><br>For Internal Authentication, the REST 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 REST 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<br>(Password management)</td><td colspan="2"><u>Objective(s)</u>: O.USER_I&A<br><br><u>Summary</u>: The TOE manages the following password.<br>• Device Administrator Password<br><br>This value is composed of any combination of upper- and lower-case letters, numbers, and the special characters specified in FIA_PMG_EXT.1. Its length 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.<br><br>The Device Administrator Password is used by the Control Panel, EWS, and REST interfaces and can be managed through the EWS.</td></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<br>(Pre-shared key composition)</td><td colspan="2"><u>Objective(s)</u>: O.COMMS_PROTECTION<br><br><u>Summary</u>: The TOE supports IPsec text-based pre-shared keys and accepts bit-based pre-shared keys.<br><br>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</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 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).<br><br>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.<br><br>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.<br><br>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"><u>Objective(s)</u>: O.USER.I&A<br><br><u>Summary</u>:<br><br><u>Control Panel</u><br><br>From the Control Panel, the user can perform the following actions prior to authentication.<ul><li>View the Welcome message</li><li>Reset the session</li><li>Select the Sign In button</li><li>Select a sign-in method from Sign In screen</li><li>View the device status information</li><li>Change the display language for the session</li><li>Place the device into sleep mode</li><li>View or print network connectivity status information</li><li>View or print Web Services status information</li></ul></td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | • View help information<br>• View the system time<br><br>The Control Panel user cannot perform any other TSF-mediated actions until after the user has been successfully authenticated.<br><br>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.<br>• Internal Authentication method<br>  ○ Local Device Sign In<br>• External Authentication methods<br>  ○ LDAP Sign In<br>  ○ Windows Sign In (via Kerberos)<br><br>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.<br><br>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.<br><br>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.<br><br>*Network interfaces*<br><br>Most of the client network interfaces protected by IPsec perform authentication. Table 53 provides a list of the available IPsec client interfaces to the TOE, whether or not there is an authentication mechanism associated with the client interface, and a list of TSF-mediated actions prior to authentication, if any. |

**Table 53: IPsec client interfaces**

| IPsec client interface | Authentication? | TSF-mediated actions prior to authentication? |
|---|---|---|
| PJL (a.k.a. P9100) | No | n/a |
| EWS | Yes | Select a sign in method |
| REST | Yes | • Discover a subset of the Web Services<br>• Obtain the X.509v3 certificate on the print engine<br>• Obtain the secure configuration settings on the print engine<br>• Obtain list of installed licenses<br>• Install a digitally signed license<br>• Delete a license (if the license in the payload of the request is digitally signed)<br>• Obtain Web Services registration status<br>• Obtain printer Claim Code for Web Services registration<br>• Set printer Claim Code for Web Services registration |

*PJL over IPsec*

PJL provides all client computers with a non-administrative network interface for submitting print jobs. The PJL interface uses the username provided in the print job as the user identifier for the print job on the TOE. Thus, print jobs stored on the TOE will be owned by this username. This username is by default the username of the human user signed in to the client computer, but it is possible for the human user submitting the print job to provide a different username for the

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | print job. The TOE does not require authentication of this username. Table 53 shows any TSF-mediated actions prior to authentication for this protocol.<br><br>*EWS over IPsec*<br><br>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 53 shows any TSF-mediated actions prior to authentication for this protocol.<br><br>*REST over IPsec*<br><br>The REST interface is an administrative interface used to manage the TOE over IPsec.<br><br>The REST 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 REST interface supports the Windows Sign In method which requires the user to be associated with the Device Administrator permission set. Table 53 shows any TSF-mediated actions prior to authentication for this protocol.<br><br>*Other*<br><br>Also see the TSS for FIA_UID.1.<br><br>**Note:** On models that support a fax phone line, the fax phone line connection does not support I&A. | |
| | 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).* |
| | Resp | 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.<br><br>Over the IPsec channel, EWS provides the same sign in methods as the Control Panel. The REST interface provides the Local Device Sign In and Windows Sign In methods. |
| | AA | *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).* |
| | Resp | The Control Panel, EWS, and REST interfaces perform I&A. |
| | AA | *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.* |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></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.<ul><li>View the Welcome message</li><li>Reset the session</li><li>Select the Sign In button</li><li>Select a sign-in method from Sign In screen</li><li>View the device status information</li><li>Change the display language for the session</li><li>Place the device into sleep mode</li><li>View or print network connectivity status information</li><li>View or print Web Services status information</li><li>View help information</li><li>View the system time</li></ul>For EWS, the user can select a sign in method.<br>For REST, the user can perform the following actions prior to I&A:<ul><li>Discover a subset of the Web Services</li><li>Obtain the X.509v3 certificate on the print engine</li><li>Obtain the secure configuration settings on the print engine</li><li>Obtain list of installed licenses</li><li>Install a digitally signed license</li><li>Delete a license (if the license in the payload of the request is digitally signed)</li><li>Obtain Web Services registration status</li><li>Obtain printer Claim Code for Web Services registration</li><li>Set printer Claim Code for Web Services registration</li></ul></td></tr>
<tr><td>FIA_UAU.7 (Protected authentication feedback)</td><td colspan="2"><u>Objective(s)</u>: O.USER.I&A<br><br><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>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | AA | *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.* |
| | Resp | 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. |
| FIA_UID.1 (Timing of identification) | **Objective(s)**: O.ADMIN_ROLES, O.USER.I&A<br>**Summary**: From the Control Panel, the user can perform the following actions prior to identification.<br>• View the Welcome message<br>• Reset the session<br>• Select the Sign In button<br>• Select a sign-in method from Sign In screen<br>• View the device status information<br>• Change the display language for the session<br>• Place the device into sleep mode<br>• View or print network connectivity status information<br>• View or print Web Services status information<br>• View help information<br>• View or print the Web Services status information<br>• View the help information<br>• View the system time<br>Once the IPsec channel is successfully established, the following interfaces initiate their identification mechanisms. The following shows their TSF-mediated actions prior to identification.<br>• EWS:<br>o Select a sign in method<br>• REST:<br>o Discover a subset of the Web Services<br>o Obtain the X.509v3 certificate on the print engine<br>o Obtain the secure configuration settings on the print engine<br>o Obtain list of installed licenses<br>o Install a digitally signed license<br>o Delete a license (if the license in the payload of the request is digitally signed)<br>o Obtain Web Services registration status<br>o Obtain printer Claim Code for Web Services registration<br>o Set printer Claim Code for Web Services registration<br>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. | |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">For additional information on I&A, see the TSS for FIA_UAU.1.<br><br>Note: On models that support a fax phone line, the fax phone line connection does not support I&A.</td></tr>
<tr><td></td><td>AA</td><td>It is covered by the assurance activities for FIA_UAU.1.</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FIA_USB.1 (User-subject binding)</td><td colspan="2"><u>Objective(s)</u>: O.USER.I&A<br><br><u>Summary</u>:<br><br><u>Control Panel User Identity Binding</u><br><br>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.<br><br>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.<br><br>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.<br><br><u>Control Panel and EWS User Role Binding</u><br><br>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.<br><br>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.<br><br>Device Administrator session PS = Device Administrator PS.<br><br>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.<br><br>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.</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | 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.<br><br>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.<br><br>The TOE combines these various PSs using one of the following three methods.<br><br>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.<br><br>*User session PS = External user account PS + Device Guest PS.*<br><br>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.<br><br>*User session PS = Network group PSs + Device Guest PS.*<br><br>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.<br><br>*User session PS = External Authentication method PS + Device Guest PS.*<br><br>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 at the product control panel" 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.<br><br>*Remote User Identity Binding*<br><br>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.<br><br>The EWS and REST interfaces support I&A mechanisms and use some form of username (e.g., Display name, Windows username) in audit records.<br><br>In the case of EWS, the interface provides the same options as the Control Panel for sign in methods. Because of this, the EWS identity will be the Display name if the Local Device Sign In |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">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 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.<br><br>In the case of the REST 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 REST identity will be the Display name. When authenticating via the Windows Sign In Method, the REST identity will be the Windows username.<br><br>From an auditing and access control perspective, the IP address is used by IPsec when generating IPsec-related and network-related audit records. The REST identity is used for all other identity-related purposes such as management-related tasks and audit records and access control enforcement and audit records.<br><br>Note: The PJL over IPsec interface contains a print job username as part of the print job data. This username is used by the TOE as the owner of the print job object when storing the print job on the TOE. The owner is not the user identity of the client computer. The IP address of the client computer is the user identity of the client computer.<br><br><u>Remote User Role Binding</u><br><br>In the case of EWS, the role is determined by the login account used by the user when logging in to the EWS interface.<br><br>In the case of PJL, the PJL interface only supports unauthenticated users. No specific role exists for these users.<br><br>In the case of the REST interface, the role is determined by the login account used by the user when logging in to the REST interface.<br><br><u>Other</u><br><br>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.</td></tr>
<tr><td></td><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></td><td>Resp</td><td>See the explanation in the Summary section above.</td></tr>
<tr><td>FMT_MOF.1 (Management of functions)</td><td colspan="2"><u>Objective(s)</u>: O.ADMIN_ROLES<br><br><u>Summary</u>:<br><br>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</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | 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.<br><br>***Control Panel Mandatory Sign-in***: With the "Control Panel Mandatory Sign-in" 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.<br><br>***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.<br><br>***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. 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.<br><br>***Account lockout***: With the account lockout function, the TOE provides an administrator the ability to enable and disable the account lockout function 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.<br><br>***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.<br><br>***IPsec***: With the IPsec function, the TOE provides an administrator the ability to enable and disable IPsec. IPsec 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 FCS_IPSEC_EXT.1.<br><br>***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. | |
| | AA | *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.* |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | | *The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.* |
| | Resp | The required information is provided in the Summary section above. |
| FMT_MSA.1 (Management of attributes) | **Objective(s)**: O.ACCESS_CONTROL, O.USER_AUTHORIZATION<br><br>**Summary**: Depending on the interface used to access the TOE, the security attributes used by the TOE's access control mechanism described in FDP_ACF.1 vary. The easiest way to describe these attributes is to split them into the following categories.<br>• Control Panel and EWS subject attributes (identities and roles)<br>• Job Storage object attributes<br><br>*Control Panel and EWS identities*<br><br>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.<br><br>The TOE supports both Internal and External Authentication mechanisms in the evaluated configuration.<br><br>***Account identity (Internal Authentication mechanism)***: The Internal Authentication mechanism 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 Display name could be used by the access control mechanism to compare job ownership and fax ownership identities, but since this account has the Device Administrator permission set permanently associated with it, this account 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 33. Because there are no management operations, the authorized roles entry is marked as not applicable (n/a) in Table 33. There is no default value property for the Display name because the account is predefined, thus, Table 33 shows this as not applicable (n/a). Similarly, no role can override the default value.<br><br>***Account identity (External Authentication mechanisms)***: 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 (a.k.a. jobs) 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 33. Because the TOE has no control over these external account identities, there is no default value property (marked as n/a in Table 33) and no default value to override, thus, no role can override the default value.<br><br>*Control Panel and EWS roles*<br><br>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 | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | 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 (a.k.a. jobs) on the TOE.<br><br>***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.<br><br>***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.<br><br>***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.<br><br>*Job Storage ownerships*<br><br>Ownership (job owner, fax owner) of Job Storage objects is assigned as the object enters the TOE. The TOE does not provide a method to modify the ownership of an object after the object is created. Only authenticated users can access the Job Storage area.<br><br>***Job owner***: For job ownership (excluding receive fax ownership), the TOE provides the "view" ownership management operation. This operation is available to the job owner and U.ADMIN. There is no default value property for a non-receive fax job. The owner is either a Control Panel user or it is the owner specified in a print job submitted over the PJL interface. Because there is no default value property, there is no role that can override the default value property.<br><br>***Fax owner***: For receive fax ownership, the TOE provides the "view" ownership management operation. This operation is available to U.ADMIN only. By default, all receive faxes are owned by the Device Administrator account. This default value property is considered restrictive because only a U.ADMIN can access a receive fax job. This default value property cannot be overridden, therefore, there is no role that can override this default value. | |
| | AA | *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.* |
| | Resp | n/a |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| FMT_MSA.3 (Initialization of attributes) | **Objective(s)**: O.ACCESS_CONTROL, O.USER_AUTHORIZATION<br>**Summary**: The descriptions have been provided in the TSS for FMT_MSA.1. | |
| | AA | *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.* |
| | Resp | The descriptions have been provided in the TSS for FMT_MSA.1. |
| FMT_MTD.1 (Management of TSF data) | **Objective(s)**: O.ACCESS_CONTROL<br>**Summary**:<br>*TSF Data owned by U.NORMAL or associated with Documents or jobs owned by a U.NORMAL*<br>**None:** U.NORMAL does not own any TSF Data on the TOE. The security attributes associated with Documents or jobs owned by U.NORMAL are covered by FMT_MSA.1.<br>*List of TSF Data not owned by U.NORMAL*<br>***Device Administrator password***: For the Device Administrator password, the TOE provides the "change" operation. The change operation allows a 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.<br>***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.<br>***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 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.<br>**Note:** Although audit records are TSF Data not owned by U.NORMAL, the TOE does not provide the ability to management audit records.<br>*List of software, firmware, and related configuration data*<br>***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.<br>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 | |

| TOE SFRs | TOE SFR compliance rationale |
|---|---|
| | identity certificate to the TOE. The delete operation removes the CA-signed identity certificate from the TOE. These operations are restricted to U.ADMIN.<br><br>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.<br><br>***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.<br><br>***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.<br><br>***Minimum password length***: For the minimum password length settings, the TOE provides the "change" operation. The TOE provides minimum password length setting for the Device Administrator account. This operation is restricted to U.ADMIN. For related information, see the TSS for FIA_PMG_EXT.1.<br><br>***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 reset 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 attempts value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1.<br><br>***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 |

<table>
<tr><th>TOE SFRs</th><th colspan="2">TOE SFR compliance rationale</th></tr>
<tr><td></td><td colspan="2">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.<br><br>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.<br><br>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.</td></tr>
<tr><td></td><td>AA</td><td>None</td></tr>
<tr><td></td><td>Resp</td><td>n/a</td></tr>
<tr><td>FMT_SMF.1 (Management functions)</td><td colspan="2"><u>Objective(s)</u>: O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION<br><br><u>Summary</u>: Table 35 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.<br><br>The following objectives do not have security management functionality defined for them in this ST.<br>• O.FAX_NET_SEPARATION<br>• O.KEY_MATERIAL<br>• O.STORAGE_ENCRYPTION<br>• O.TSF_SELF_TEST<br>• 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</td><td colspan="2"><u>Objective(s)</u>: O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION</td></tr>
</table>

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| (Security roles) | **Summary**: The TOE supports two roles:<br>• U.ADMIN<br>• U.NORMAL<br><br>The TOE can associate users with roles, but there is an account that is always associated with a specific role. Specifically, the Device Administrator account (available through the Control Panel, EWS, and REST interfaces) is of type U.ADMIN.<br><br>*Permission sets*<br><br>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.<br><br>The TOE contains the following built-in permission sets.<br>• Device Administrator—Grants administrative capabilities<br>• Device User—Grants typical user capabilities<br>• Device Guest—Grants capabilities to non-signed in users<br><br>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.)<br><br>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.<br><br>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.)<br><br>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.<br><br>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. | |
| | AA | *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.* |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | Resp | n/a |
| FPT_KYP_EXT.1<br>(Key chain key protection) | **Objective(s)**: O.KEY_MATERIAL<br><br>**Summary**: As per FCS_KYC_EXT.1/CDE, the key chain for Customer Data Encryption contains intermediate keys that are either derived or encrypted. The keys consist of the passphrase, derived key, and volume key. The passphrase is generated by the TSF when the HCD is powered on for the first time and is used as input into the PBKDF2 to generate the derived key that is used to encrypt/decrypt the volume key. The volume key is used to encrypt/decrypt customer data partition on the eMMC drive. The passphrase is stored in non-field replaceable nonvolatile storage (NVRAM) located inside the TOE. The derived key is stored in RAM and is destroyed when the TOE is powered off. The volume key is stored in encrypted form on the eMMC drive. For more information on the key chain, see the TSS for FCS_KYC_EXT.1/CDE.<br><br>As per FCS_KYC_EXT.1/CM, the key chain for certificate management is a key chain of one consisting of the data encryption key. The data encryption key is generated by the TSF when the HCD is powered on for the first time and is used to encrypt/decrypt identity certificates and their corresponding private keys on the eMMC drive. The data encryption key is stored in non-field replaceable nonvolatile storage (NVRAM) located inside the TOE. For more information on the key chain, see the TSS for FCS_KYC_EXT.1/CM.<br><br>As per FCS_KYC_EXT.1/JCF, the key chain for encrypting/decrypting the JDI configuration file contains intermediate keys that are combined to generate the data encryption key. The keys consist of the intermediate key, submasks, and data encryption key. The intermediate key is generated when the HCD is powered on for the first time and is combined with submasks (e.g., MAC address, serial number) in order to generate the data encryption key. The data encryption key is used to encrypt/decrypt the JDI configuration file. The intermediate key and submasks are stored in  in non-field replaceable nonvolatile storage (NVRAM) located inside the TOE. The data encryption key is stored in RAM and is destroyed when the TOE is powered off. For more information on the key chain, see the TSS for FCS_KYC_EXT.1/JCF. | |
| | AA | *None* |
| | Resp | n/a |
| FPT_SKP_EXT.1<br>(Key viewing protection) | **Objective(s)**: O.COMMS_PROTECTION<br><br>**Summary**: 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.<br><br>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.<br><br>The TOE stores the IPsec pre-shared keys in a file on the eMMC drive. 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. | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | 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.<br><br>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. | |
| | AA | *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.* |
| | Resp | 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. |
| FPT_STM.1<br>(Time stamps) | **Objective(s)**: O.AUDIT<br><br>**Summary**: 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.<br><br>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. | |
| | AA | *The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.* |
| | Resp | The TOE contains an internal system clock that is synchronized using an NTS. |
| FPT_TST_EXT.1<br>(TSF testing) | **Objective(s)**: O.TSF_SELF_TEST<br><br>**Summary**: The TOE contains TSF testing functionality called Whitelisting to help ensure only authentic, known-good firmware files that have not been tampered with are loaded into memory.<br><br>The TOE supports dm-verity to protect the integrity of the SquashFS file system firmware images. On each boot, the TOE verifies the digital signature of the dm-verity hash tree corresponding to a SquashFS file system image using RSA-2048 with SHA2-256. During operation, the TOE verifies the integrity of a file system block before loading it into memory.<br><br>If the digital signature verification fails, or the integrity check of a file system block 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.<br><br>Whitelisting uses the HP FutureSmart Firmware OpenSSL 1.1.1 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). | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | AA | *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.* |
| | Resp | The TOE performs Whitelisting of the SquashFS file system firmware images while booting. If digital signature verification fails of a dm-verity hash tree corresponding to any of the SquashFS file system firmware images, or the integrity check of file system block fails, 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. |
| FPT_TUD_EXT.1 (Trusted update) | **Objective(s)**: O.UPDATE_VERIFICATION<br><br>**Summary**: The TOE's firmware can be updated by an administrator by downloading an update image and installing it on the TOE.<br><br>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.<br><br>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 will not allow the update to proceed. The TOE uses the HP FutureSmart Firmware OpenSSL 1.1.1 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.<br><br>The current version of both the System firmware and the Jetdirect Inside firmware can be obtained through the following interfaces.<br>• Control Panel<br>• EWS<br><br>How to obtain the firmware versions using the EWS is described in the [CCECG] section *Check version of installed TOE firmware*.<br><br>**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. | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | AA | *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.*<br><br>*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.* |
| | Resp | 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.<br><br>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.<br><br>The current version of both the System firmware and the Jetdirect Inside firmware can be obtained through the following interfaces.<br>• Control Panel<br>• EWS |
| FTA_SSL.3 (Interactive session termination) | **Objective(s)**: O.USER_I&A<br><br>**Summary**: This SFR applies to the interactive sessions for the Control Panel and EWS. The TOE's REST interfaces do not support the concept of sessions.<br><br>*Control Panel*<br><br>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 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.<br><br>*EWS*<br><br>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. | |
| | AA | *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.* |
| | Resp | All Control Panel and EWS sessions support session termination. Both have administratively configurable timeout periods. |
| FTP_ITC.1 | **Objective(s)**: O.AUDIT, O.COMMS_PROTECTION | |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| (Trusted channel) | **Summary**: 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.<br><br>The TOE provides and initiates trusted communication channels to the following authorized IT entities.<br>• authentication server<br>• DNS server<br>• FTP server<br>• NTS server<br>• SharePoint server<br>• SMB server<br>• SMTP server<br>• syslog server (audit server)<br>• WINS server<br><br>For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1. | |
| | AA | *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.* |
| | Resp | All trusted communications channels to authorized IT entities use IPsec. |
| FTP_TRP.1(a) (Administrator trusted path) | **Objective(s)**: O.COMMS_PROTECTION<br><br>**Summary**: 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.<br><br>The following interfaces are the remote administrative interfaces of the TOE in the evaluated configuration.<br>• EWS (via a web browser)<br>• REST<br><br>For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1. | |
| | AA | *The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected.* |

| TOE SFRs | TOE SFR compliance rationale | |
|---|---|---|
| | | *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.* |
| | Resp | All remote administrative interfaces use IPsec. The remote administrative interfaces are EWS and REST. |
| FTP_TRP.1(b) (User trusted path) | **Objective(s)**: O.COMMS_PROTECTION<br>**Summary**: The TOE uses IPsec to provide a trusted communication path between itself and remote, non-administrative users. 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.<br>The TOE supports the connection of multiple remote non-administrative users. The following interface is the remote non-administrative interface of the TOE in the evaluated configuration.<br>• PJL<br>For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1. | |
| | AA | *The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-administrative users are indicated, along with how those communications are protected.*<br>*The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are consistent with those specified in the requirement, and are included in the requirements in the ST.* |
| | Resp | All remote non-administrative users connect through the PJL interface. The TOE requires all PJL connections to use IPsec. |

# 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 |
| 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 |
| PJL | Printer Job Language |
| PKCS | Public-Key Cryptography Standards |
| PP | Protection Profile |
| PS | Permission Set |
| PSK | Pre-Shared Key |
| PSTN | Public Switched Telephone Network |
| REST | Representational State Transfer |
| RFC | Request for Comments |
| RSA | Rivest-Shamir-Adleman |
| SA | Security Association |
| SAR | Security Assurance Requirement |
| SATA | Serial AT Attachment |
| SED | Self-Encrypting Drive |
| SFP | Single-Function Printer |
| 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) |
| SPI | Serial Peripheral Interface |
| 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 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, REST, 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 Security Target. |
| 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** **Common Criteria Evaluated Configuration Guide for HP Multifunction Printers**

**HP Color LaserJet Enterprise MFP M480**
**HP Color LaserJet Managed MFP E47528**
**HP LaserJet Enterprise MFP M430/M431**
**HP LaserJet Managed MFP E42540**

Author(s) HP Inc.

Edition 1

Date 5/2023

**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

**CCEVS-TD0253** **Assurance Activities for Key Transport**

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

**CCEVS-TD0474** **Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1**

Date 2019-12-04

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0474

**CCEVS-TD0494** **Removal of Mandatory SSH Ciphersuite for HCD**

Date 2020-02-20

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0494

**CCEVS-TD0562** **Test activity for Public Key Algorithms**

Date 2021-01-27

Location https://m.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0562

**CCEVS-TD0642** **FCS_CKM.1(a) Requirement; P-384 keysize moved to selection**

Date 2022-06-17

Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0642

**E42540_UG** **HP LaserJet Managed MFP E42540**

**User Guide**

Author(s) HP Inc.

Edition 2

Date 2/2021

**E47528_UG** **HP Color LaserJet Managed MFP E47528**

**User Guide**

Author(s) HP Inc.

Edition 2

Date 2/2021

| | | |
|---|---|---|
| **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 | 2008-07-16d |
| | 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/MMO/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 and Samsung Hardcopy Devices with 5.3.2 Firmware and Linux 4.9.180** | |
| | Author(s) | HP Inc. |
| | Version | 1.1 |
| | Date | 2023-03-08 |

**M42540-47528_IG** **HP LaserJet Managed MFP E42540**
**HP Color LaserJet Managed MFP E47528**

**Installation Guide**

Author(s) HP Inc.

Date 2020

**M430-31_UG** **HP LaserJet Enterprise MFP M430, M431**

**User Guide**

Author(s) HP Inc.

Edition 2

Date 2/2021

**M430-31-480_IG** **HP LaserJet Enterprise MFP M430, M431**
**HP Color LaserJet Enterprise MFP M480**

**Installation Guide**

Author(s) HP Inc.

Date 2020

**M480-UG** **HP Color LaserJet Enterprise MFP M480**

**User Guide**

Author(s) HP Inc.

Edition 2

Date 2/2021

**QuickSec73** **IPsec Toolkit Feature Guide**

**Release 7.3**

Author(s) INSIDE Secure

Date December 5, 2018

**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

**RFC4304** **Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)**

Author(s) S. Kent

Date December 2005

Location https://www.ietf.org/rfc/rfc4304.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-Rev2** **Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography**

Date May 2013

Location https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

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

Date April 2018

Location https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

**SP800-90A-Rev1** **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**

Date June 2015

Location https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf