HP LaserJet Enterprise 8501

Security Target

Version:	**1.11**
Classification:	**Public**

Trademarks

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

- HP®

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 Rambus Inc. in the United States, other countries, or both.

- Rambus®
- 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.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Version	Date	Author(s)	Description
1.11	2025-12-03	HP Inc.	Initial public version.

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

Title:	**HP LaserJet Enterprise 8501** **Security Target**
Version:	1.11
Date:	2025-12-03
Sponsor:	HP Inc.
Developer:	HP Inc.
Certification Body:	OCSI
Certification ID:	OCSI/CERT/ATS/09/2025
Keywords:	Common Criteria, HCD, Hardcopy Device, LaserJet, LaserJet Enterprise, 8501

1.2 TOE Identification

The TOE is the HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 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 single-function printer (SFP).

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 collaborative Protection Profile for Hardcopy Devices, Version 1.0e, dated 4 March 2024 [HCDcPP].

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

Both firmware modules run on top of the same Linux 5.10 operating system.

The System firmware controls all functionality except for the network-related functionality and functionality implemented by the operating system. The Jetdirect Inside firmware controls the network-related functionality from Ethernet to Internet Key Exchange (IKE). These firmware modules and the operating system 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, print speed, the number of output bins, and whether they contain a stapler/stacker.

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

As per [HCDcPP] Section 1.4.4, the major security functions in this evaluation are as follows.

- Identification, authentication, and authorization to use HCD functions
- Access control
- Encryption
- Trusted communications
- Administrative roles
- Auditing
- Trusted operation

1.4.1 Required and Optional Hardware, Software, and Firmware

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

- One administrative client computer network connected to the TOE in the role of an Administrative Computer.
- Web browser installed on the administrative client computer network connected to the TOE in the role of an Administrative Computer
- A Domain Name System (DNS) server
- A Network Time Service (NTS) server
- A Windows Internet Name Service (WINS) server
- A Syslog server
- One or both of the following:
  - A Lightweight Directory Access Protocol (LDAP) server
  - A Windows domain controller/Kerberos server
- At least one OCSP responder capable of processing OCSP requests originating from the TOE

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)
- The following remote file systems:
  - Server Message Block (SMB)
- A Simple Mail Transfer Protocol (SMTP) gateway

1.4.2 Intended Method of Use

This evaluation covers an information processing environment in which a basic level of document security, network security, and security assurance are required.

The TOE is intended to be used in non-hostile, networked environments where TOE users have direct physical access to the HCDs for storing and printing 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 the HCD’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 [HCDcPP] Section 1.4 "TOE Use Case" supported by the TOE.

- Required use cases
    - Printing
    - Configuration
    - Auditing
    - Verifying firmware/software updates
    - Verifying HCD function
- Conditionally mandatory use cases
    - Storing and retrieving Documents
    - 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 and firmware versions included in this evaluation and provides a mapping of these HCD models and firmware versions.

Table 1: TOE hardware and firmware reference

Product model name	Product number	Product model name (Name displayed in the EWS)	System firmware version	Jetdirect Inside firmware version
HP LaserJet Enterprise 8501	9S187A	HP LaserJet 8501	2509306_000339	JOL25090252
	AJ7J3A			
	AQ1E4A			
	BD5H0A			
	BH6N7AV			

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 Single-function Printers HP LaserJet Enterprise 8501 Edition 1, 1/2026	[CCECG]

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

Table 3: TOE OS and processor

Item	Type
OS	Linux 5.10
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 and storing of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration except when the administrator performs trusted update via the USB).

[HCDcPP] 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 5.10 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 Linux operating system implements IPsec using its XFRM framework. The Jetdirect Inside firmware implements Internet Key Exchange version 2 (IKEv2) and supports X.509v3 certificate-based authentication. The TOE supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), although IPv6 is disabled in the evaluated configuration.

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.

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.

SMB

The TOE supports a remote file system for storing and retrieving backup files during Back up and Restore operations. The TOE uses IPsec to protect the communication to the remote file system. For remote file system connectivity, the TOE supports the SMB protocol.

SMTP mail server

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 the servers over an IPsec connection.

Control Panel

Each HCD contains a user interface (UI) called the Control Panel which consists of a touchscreen LCD. 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 [HCDcPP] 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 a self-encrypting Solid State Drive (SSD).

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

Firmware Components

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both of these firmware components share the same operating system (Linux 5.10). These firmware components and the operating system work together to provide the security functionality defined in this document for the TOE.

The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the System firmware. The Jetdirect Inside firmware includes IKE 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 device to print jobs.

The operating system implements dm-verity, dm-crypt, IPsec, and includes the HP FutureSmart Firmware Linux Kernel Crypto API which implements cryptographic algorithms relied upon by TOE security functionality (e.g.., IPsec).

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 Encryption

1.5.3.2.1 IPsec

The TOE's IPsec supports X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange version 2 (IKEv2) 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), Secure Hash Algorithm-based (SHA-based) Hashed Message Authentication Codes (HMACs), Public-Key Cryptography Standards (PKCS) #1 v1.5 signature generation and verification, counter mode deterministic random bit generator using AES (CTR_DRBG (AES)) for IKE negotiations, and HMAC_DRBG(HMAC-SHA2-256) deterministic random bit generator for IPsec ESP.

It supports multiple DH groups, transport mode, and uses Main Mode for Phase 1 exchanges in IKEv2. IKEv2 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. IKEv2 uses imported RSA-based X.509v3 certificates to authenticate the connections. The RSA authentication is accomplished using the IKEv2 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 SSD. The TOE performs encryption of User Document Data and confidential TSF data on the SSD without any user intervention.

Customer Data Encryption

The TSF implements a feature called customer data encryption, which encrypts the partitions on the storage device designated for customer data. In the evaluated configuration, this feature is configured to use AES-CBC-256 to encrypt these partitions.

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

On every HCD boot, the customer partitions (LUKS-encrypted volumes) are recreated and reformatted. This process effectively performs a cryptographic erase of all data previously stored on these partitions.

Certificate Data Encryption

The TSF encrypts identity certificates, and their corresponding private keys stored on the storage device.

Certificates XML file:

The TSF stores the IPsec identity certificate and its corresponding private key in encrypted form in a certificates XML file stored on the storage device. AES-CBC-256 is used to encrypt the IPsec 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 storage device. AES-CBC-256 is used to encrypt thumbprint files.

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 1.5.3.7.

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 [HCDcPP] cryptographic requirements.

Table 4: TOE cryptographic implementations

Cryptographic implementation	Version	Usage
HP FutureSmart Firmware OpenSSL 1.1.1	5.9.2.1	Trusted update
		TSF testing
		Certificates XML file encryption
		Thumbprint files encryption
		RSA key pair generation during CSR creation
HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2)	5.9.2.1	Secure boot
HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	5.9.2.1	IKE
HP FutureSmart Firmware Linux Kernel Crypto API	5.10	IPsec
		Customer data encryption
		TSF testing

Cryptographic implementation	Version	Usage
Security Sub-System (SSS)	8.2	Secure boot

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) 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, etc.) 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 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 SSD. 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 IKEv2 and transport mode. The TOE supports X.509v3 certificates for endpoint authentication. For additional details on the TOE's IPsec implementation, 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 firmware bundles can be downloaded from the HP Inc. website to update the TOE’s firmware. These updates are digitally signed by HP Inc. using the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 signature scheme. The TOE's EWS interface allows an administrator to install the firmware bundles. Before installation, the TSF verifies the digital signature of the firmware bundle to ensure its integrity and authenticity. For additional details, see the TSS for FPT_TUD_EXT.1.

The TOE’s secure boot function includes an immutable hardware root of trust implemented in ROM. When power is applied to the HCD, the boot ROM executes first and verifies the integrity of the initial boot stage, which resides outside the root of trust. Each subsequent stage in the boot process then validates the integrity of the next, establishing a continuous chain of trust. The integrity of each boot stage is verified by checking its digital signature using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5. For additional details, see the TSS for FPT_SBT_EXT.1.

The TOE supports dm-verity to verify the integrity of SquashFS filesystem firmware images, helping ensure the correct operation of the TSF during startup. At each boot, the TSF verifies the digital signature of the dm-verity root hash corresponding to a SquashFS firmware image. During operation (including boot time), dm-verity checks the integrity of each filesystem block before loading it into memory by comparing it to the authenticated hash tree. The digital signature is verified using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5. For additional details, see the TSS for FPT_TST_EXT.1.

1.5.4 TOE Boundaries

1.5.4.1 Physical Boundary

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

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.

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.

- Only one Administrative Computer is used to manage the TOE.
- Third-party solutions must not be installed on the TOE.
- 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.
- HP Jetdirect XML Services must be disabled.
- External file system access through PJL and PS must be disabled.
- Only X.509v3 certificates are supported methods for IPsec authentication (IPsec authentication using pre-shared keys 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.
- HP Workpath Platform must be disabled.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- Firmware updates through REST Web Services is disallowed.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- FIPS-140 must be disabled.
- Partial clean functionality of the TOE is disallowed.
- Smart Cloud Print must be disabled.
- IPv6 addressing must be disabled.
- All stored jobs must be assigned a Job PIN or Job Encryption Password.

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 Profile:

- [HCDcPP]: collaborative Protection Profile for Hardcopy Devices, Version 1.0e, dated 4 March 2024; 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 collaborative Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community ([HCDcPP])

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
TD0926	HIT Technical Decision: Clarification on FPT_SBT_EXT.1 Root of Trust	Applicable.	[CCEVS-TD0926]
TD0927	HIT Technical Decision: Clarification on FPT_KYP_EXT.1 when using TPM-like device	Applicable.	[CCEVS-TD0927]
TD0928	HIT Technical Decision: FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 Time based test case as optional	Not applicable. Neither FCS_SSHC_EXT.1.8 nor FCS_SSHS_EXT.1.8 is claimed.	[CCEVS-TD0928]
TD0937[1]	CPP_HCD_V1.0 Endorsement Requirements	Applicable.	[CCEVS-TD0937]

[1] A Technical Query has been submitted to the NIAP Technical Rapid Response Team (TRRT) concerning this NIAP TD. The NIAP TRRT response is currently pending.

3 Security Problem Definition

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

3.1 Users

There are two categories of Users defined in this Security Target:

1. Normal User [U.NORMAL] is a user who has been identified and authenticated and does not have an administrative role.
2. Administrator [U.ADMIN] is a user who has been identified and authenticated and has an administrative role.

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

3.2 Assets

Assets are passive entities in the TOE that contain or receive information. In the HCDcPP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in the HCDcPP:

1. User Data [D.USER] which are data created by and for Users that do not affect the operation of the TSF.
2. TSF Data [D.TSF] which are data created by and for the TOE that might affect the operation of the TSF.

3.2.1 User Data

User Data are composed of two types:

1. User Document Data [D.USER.DOC] which is information contained in a User's Document, in electronic or hardcopy form.
2. User Job Data [D.USER.JOB] which is information related to a User's Document or Document Processing Job.

3.2.2 TSF Data

TSF Data are composed of two types:

1. Protected TSF Data [D.TSF.PROT] which are TSF data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable.
2. Confidential TSF Data [D.TSF.CONF] which are TSF data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE.

3.3 Threats

Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 7: Threats

Threat	Definition
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 or the physical Nonvolatile Storage component.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_FAILURE	A malfunction of the TSF may compromise the device security status if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may install unauthorized firmware/software on the TOE to modify the Device security status.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.
T.WEAK_CRYPTO	An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes to access (read, modify, or delete) TSF and User data.

3.4 Organizational Security Policies

Organizational Security Policies are used to provide a basis for Security Objectives that are not practical to define on the basis of Threats to Assets or that originate primarily from customer expectations.

Table 8: Organizational security policies

Organizational security policy	Definition
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 stored within the TOE as well as 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 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 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.

Organizational security policy	Definition
P.ROT_INTEGRITY	The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.

3.5 Assumptions

Assumptions are conditions that must be satisfied in order for the Security Objectives and functional requirements to be effective.

Table 9: Assumptions

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

4 Security Objectives

4.1 Security Objectives for the TOE

Table 10: 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 firmware/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 store it internally as well as be capable of sending it to a trusted External IT Entity.
O.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data in 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 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.AUTH_FAILURES	The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.

Security objective	Description
O.FW_INTEGRITY	The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.
O.STRONG_CRYPTO	The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

4.2 Security Objectives for the Operational Environment

Table 11: 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 security objectives to threats, assumptions, and organizational security policies (OSPs), showing that each objective counters or enforces at least one threat, assumption, or OSP.

Table 12: Mapping of security objectives to threats, assumptions, or OSPs

Security Objective	Threat, Assumption, or OSP
O.USER_I&A	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUTHORIZATION

Security Objective	Threat, Assumption, or OSP
O.ACCESS_CONTROL	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUDIT
O.USER_AUTHORIZATION	P.AUTHORIZATION P.AUDIT
O.ADMIN_ROLES	T.UNAUTHORIZED_ACCESS T.TSF_COMPROMISE P.AUTHORIZATION
O.UPDATE_VERIFICATION	T.UNAUTHORIZED_UPDATE
O.TSF_SELF_TEST	T.TSF_FAILURE
O.COMMS_PROTECTION	T.NET_COMPROMISE P.COMMS_PROTECTION
O.AUDIT	P.AUDIT
O.STORAGE_ENCRYPTION	P.STORAGE_ENCRYPTION
O.KEY_MATERIAL	P.KEY_MATERIAL
O.AUTH_FAILURES	T.UNAUTHORIZED_ACCESS
O.FW_INTEGRITY	P.ROT_INTEGRITY
O.STRONG_CRYPTO	T.WEAK_CRYPTO
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

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

Table 13: Mapping of security objectives for the Operational Environment to assumptions, threats and OSPs

Objective	Assumptions/Threats/OSPs
OE.PHYSICAL_PROTECTION	A.PHYSICAL

Objective	Assumptions/Threats/OSPs
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 14: 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. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. O.AUTH_FAILURES resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
T.TSF_COMPROMISE	O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users. O.USER_I&A provides the basis for access control. O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.
T.TSF_FAILURE	O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.
T.WEAK_CRYPTO	O.STRONG_CRYPTO implements strong cryptographic mechanisms to provide sufficient resistance to current attack capabilities.
T.UNAUTHORIZED_UPDATE	O.UPDATE_VERIFICATION verifies the authenticity of firmware/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 15: Sufficiency of objectives holding assumptions

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

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 16: 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. O.USER_I&A provides the basis for authorization. O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.
P.AUDIT	O.AUDIT requires the generation of audit data. O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users. O.USER_AUTHORIZATION provides the basis for authorization.
P.COMMS_PROTECTION	O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.
P.STORAGE_ENCRYPTION	O.STORAGE_ENCRYPTION protects User Document Data and Confidential TSF Data stored in Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.

OSP	Rationale for security objectives
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.ROT_INTEGRITY	O.FW_INTEGRITY ensures that the TOE's own integrity remains intact and can attest its integrity to outside parties on request.

5 Extended Components Definition

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

5.1 Security Audit (FAU)

5.1.1 FAU_STG_EXT Extended: External Audit Trail Storage

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 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management

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

There are no auditable events foreseen.

5.1.1.1 FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components

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

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

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

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

5.2 Cryptographic Support (FCS)

5.2.1 FCS_CKM_EXT Extended: Cryptographic Key Management

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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.1.1 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to:	No other components
Dependencies:	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
FCS_CKM_EXT.4.1	The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.
Rationale	Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction. This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.2.2 FCS_IPSEC_EXT Extended: IPsec selected

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

There are no management activities foreseen.

Audit

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

a) Failure to establish an IPsec SA.

5.2.2.1 FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to:	No other components
Dependencies:	FCS_CKM.1 Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/DataEncryption Cryptographic operation (Data Encryption/decryption) FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification) FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm) FCS_RBG_EXT.1 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 have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: *transport mode, tunnel mode*].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: *AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106),*] together with a Secure Hash Algorithm (SHA)-based HMAC [selection: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, no HMAC algorithm*].

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 RFC 5996, 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 [selection: *AES-CBC-128, AES_CBC-192, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282)*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

• *IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [selection:*

○ *number of bytes;*

○ *length of time, where the time values can be configured within [assignment: integer range including 24] hours;*];

• *IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection:*

○ *number of bytes;*

○ *length of time, where the time values can be configured within [assignment: integer range including 24] hours*]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

• *IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [selection:*

○ *number of bytes;*

○ *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*];

• *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [selection:*

○ *number of bytes;*

○ *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*]

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: (one or more) number(s) of bits that is at least twice the security strength of the negotiated Diffie-Hellman group] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: *IKEv1, IKEv2*] exchanges of length [selection:

• *according to the security strength associated with the negotiated Diffie-Hellman group;*

- *at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- *[selection: 14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP)] according to RFC 3526,*
- *[selection: 19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (521-bit Random ECP), 24 (2048- bit MODP with 256-bit POS)] according to RFC 5114.*

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 1, IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: *IKEv1 Phase 2, IKEv2 CHILD_SA*] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [selection: *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [selection: *Preshared Keys, no other method*].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, Distinguished Name (DN)*] and [selection: *no other reference identifier type, [assignment: other supported reference identifier types]*].

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 FCS_KDF_EXT 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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.3.1 FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Hierarchical to:	No other components
Dependencies:	FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication), FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction [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, ISO/IEC 11770-6:2016 [selection: KPF2, KPF3, KPF4]*], using the keyed-hash functions specified in FCS_COP.1/CMAC, such that the output is at least of equivalent security strength (in number of bits) to the BEV or the DEK.
Rationale	The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions. This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.2.4 FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.4.1 FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to:	No other components
Dependencies:	[FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping), FCS_SMC_EXT.1 Extended: Submask Combining, FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction, FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption), FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1/KeyTransport Cryptographic operation (Key Transport)].
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/KeyWrap, key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1/KeyEnc, key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1/KeyTransport*]] 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 FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

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

There are no management activities foreseen.

Audit

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

b) Minimal: failure of the randomization process.

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 ISO/IEC 18031:2011 using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG ([selection: AES, SEED, HIGHT, LEA])*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: *[assignment: number of firmware/software-based sources] firmware/software-based noise source, [assignment: number of hardware-based sources] hardware based noise source*] with a minimum of [selection: *128 bits, 192 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18vv031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

Rationale Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.2.6 FCS_SMC_EXT 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 or the DEK.

Component levelling

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

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.6.1 FCS_SMC_EXT.1 Extended: Submask Combining

Hierarchical to:	No other components
Dependencies:	FCS_COP.1/Hash 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, BEV or DEK.
Rationale	Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV or the DEK. 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 User Data Protection (FDP)

5.3.1 FDP_DSK_EXT Extended: Protection of Data on Disk

Family behaviour

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

Component levelling

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

Management

There are no management activities foreseen.

Audit

There are no auditable 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/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
FDP_DSK_EXT.1.1	The TSF shall [selection: *perform encryption in accordance with FCS_COP.1/StorageEncryption, use a self-encrypting Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*] such that any Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.
FDP_DSK_EXT.1.2	The TSF shall encrypt all protected data without user intervention.

Rationale

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

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

5.4 Identification and Authentication (FIA)

5.4.1 FIA_PMG_EXT Extended: Password Management

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

There are no management activities foreseen.

Audit

There are no auditable 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 Authentication using X.509 certificates (FIA_X509_EXT)

Family behaviour

This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests.

Component levelling

FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

FIA_X509_EXT.3 X509 Certificate Requests, requires the TSF to be able to generate Certificate Request Messages and validate responses.

Management

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

(a) Remove imported X.509v3 certificates
(b) Approve import and removal of X.509v3 certificates
(c) Initiate certificate requests

Audit

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

(a) Minimal: No specific audit requirements are specified.

5.4.2.1 FIA_X509_EXT.1 X.509 Certificate Validation

Hierarchical to:	No other components
Dependencies:	FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.4.2.2 FIA_X509_EXT.2 X509 Certificate Authentication

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: *DTLS, HTTPS, IPsec, TLS, SSH, [assignment: other protocols], no protocols*], and [selection: *code signing for system firmware/software updates [assignment: other uses], no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: *allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate*].

5.4.2.3 FIA_X509_EXT.3 X.509 Certificate Requests

Hierarchical to: No other components

Dependencies: FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)
FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: *device-specific information, Common Name, Organization, Organizational Unit, Country, [assignment: other information]*].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.5 Protection of the TSF (FPT)

5.5.1 FPT_SBT_EXT Extended: Secure Boot

Family behaviour

This family addresses the requirements for verifying firmware/software integrity each time that that it is powered on.

Component levelling

FPT_SBT_EXT.1 Secure Boot, uses a Root of Trust to confirm the integrity of the device's firmware/software at boot time.

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.5.1.1 FPT_SBT_EXT.1 Extended: Secure Boot

Hierarchical to:	No other components
Dependencies:	FCS_COP.1/Hash Cryptographic operation (Hash Algorithm) FCS_COP.1/SigGen Cryptographic Operation (for signature generation/verification) FCS_COP.1/KeyedHash Cryptographic Operation (for keyed-hash message authentication) FCS_COP.1/DataEncryption Cryptographic Operation (Symmetric encryption/decryption) FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption) FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication)

FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in a Root of Trust that is implemented in immutable code or a HW-based write-protection mechanism.

FPT_SBT_EXT.1.2 At boot time the TSF shall use the chain(s) of trust to confirm integrity of its firmware/software using a [selection: *hash, digital signature, message authentication*] verification method.

FPT_SBT_EXT.1.3 The TSF shall [selection: *enter maintenance mode, halt boot process, reboot the device, [assignment: another behavior of TOE]*] in the event of a boot time verification failure so that the corrupted firmware/software isn't executed.

FPT_SBT_EXT.1.4 Following failure of verification, the TSF shall provide a mechanism to: [selection: *revert to previous TOE image, reinstall TOE image, perform a factory reset, indicate a need to contact vendor support*].

FPT_SBT_EXT.1.5 The TSF shall contain [selection: *hash data, digital signature data, message authentication code, public key for digital signature, symmetric key for message authentication with confidentiality protection as defined in FPT_SBT_EXT.1.6*] in the Hardware Root of Trust.

FPT_SBT_EXT.1.6 The TSF shall make the symmetric key accessible only to the Hardware Root of Trust.

Rationale Secure Boot is to verify the integrity of the boot process starting with the hardware-anchored Root of Trust and then verifying each link in the corresponding Chain of Trust to ensure that no corrupted firmware/software is executed.

This extended component verifies the integrity of the Chains of Trusts which are TSF data, and it is therefore placed in the FPT class with a single component.

5.5.2 FPT_KYP_EXT Extended: Protection of Key and Key Material

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 Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.5.2.1 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components

Dependencies: FCS_KYC_EXT.1 Extended: Key Chaining

FPT_KYP_EXT.1.1 The TSF shall [selection:

- *not store keys in non-volatile memory*
- *only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1/KeyWrap, or encrypted, as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport*
- *only store plaintext keys that meet any one of the following criteria [selection:*
  - *the key is protected by another key that is not part of the key chain as specified in FCS_KYC_EXT.1,*
  - *the key will no longer provide access to the encrypted data after initial provisioning,*
  - *the key is a key split that is combined as specified in FCS_SMC_EXT.1, and the other half of the key split is [selection:*
    - *wrapped as specified in FCS_COP.1/KeyWrap,*
    - *encrypted as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport,*
    - *derived and not stored in non-volatile memory],*
  - *the key is [selection: used to wrap a key as specified in FCS_COP.1/KeyWrap, used to encrypt a key as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport] that is already [selection: wrapped as specified in FCS_COP.1/KeyWrap, encrypted as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport],*
  - *the non-volatile memory the key is stored on is located in a protected storage device]*

].

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

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

5.5.3 FPT_SKP_EXT Extended: Protection of TSF Data

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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.5.3.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.
Rationale	Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data. This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.5.4 FPT_TST_EXT Extended: TSF testing

Family behaviour

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

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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.5.4.1 FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to:	No other components
Dependencies:	No dependencies

FPT_TST_EXT.1.1	The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.
Rationale	TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.5.5 FPT_TUD_EXT Extended: Trusted Update

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

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.5.5.1 FPT_TUD_EXT.1 Trusted Update

Hierarchical to:	No other components
Dependencies:	[FCS_COP.1/SigGen Cryptographic Operation (for signature generation/verification), FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)].
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 [selection: *digital signature, X.509 certificate*] and [selection: *published hash, no other functions*] prior to installing those updates.

Rationale	Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6 Security Requirements

6.1 TOE Security Functional Requirements

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

Table 17: 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		[HCDcPP]	No	Yes	Yes	No
	FAU_GEN.2 User identity association		[HCDcPP]	No	No	No	No
	FAU_SAR.1 Audit review		[HCDcPP]	No	No	No	No
	FAU_SAR.2 Restricted audit review		[HCDcPP]	No	No	No	No
	FAU_STG.1 Protected audit trail storage		[HCDcPP]	No	No	No	No
	FAU_STG.4 Prevention of audit data loss		[HCDcPP]	No	No	Yes	Yes
	FAU_STG_EXT.1 Extended: Audit Trail Storage		[HCDcPP]	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)	FCS_CKM.1	[HCDcPP]	No	No	No	Yes
	FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)	FCS_CKM.1	[HCDcPP]	No	No	No	Yes
	FCS_CKM.2 Cryptographic Key Establishment		[HCDcPP]	No	No	No	Yes
	FCS_CKM_EXT.4 Extended: Cryptographic key material destruction		[HCDcPP]	No	No	No	No
	FCS_CKM.4 Cryptographic key destruction		[HCDcPP]	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_COP.1/DataEncryption Cryptographic Operation (Symmetric encryption/decryption)	FCS_COP.1	[HCDcPP]	No	No	No	Yes
	FCS_COP.1/SigGen Cryptographic Operation (for signature generation/verification)	FCS_COP.1	[HCDcPP]	No	No	Yes	Yes
	FCS_COP.1/Hash Cryptographic operation (Hash algorithm)	FCS_COP.1	[HCDcPP]	No	No	No	Yes
	FCS_COP.1/StorageEncryption Cryptographic operation (AES Data Encrypt ion/Decryption)	FCS_COP.1	[HCDcPP]	No	No	No	Yes
	FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)	FCS_COP.1	[HCDcPP]	No	No	No	Yes
	FCS_COP.1/KeyedHash Cryptographic operation (for keyed-hash message authentication)	FCS_COP.1	[HCDcPP]	No	No	Yes	Yes
	FCS_COP.1/CMAC Cryptographic operation (for keyed-hash message authentication)	FCS_COP.1	[HCDcPP]	No	No	Yes	Yes
	FCS_IPSEC_EXT.1 Extended: IPsec selected		[HCDcPP]	No	No	Yes	Yes
	FCS_KDF_EXT.1		[HCDcPP]	No	No	No	Yes
	FCS_KYC_EXT.1/CDE Extended: Key chaining	FCS_KYC_EXT.1	[HCDcPP]	Yes	No	No	Yes
	FCS_KYC_EXT.1/CM Extended: Key chaining	FCS_KYC_EXT.1	[HCDcPP]	Yes	No	No	Yes
	FCS_KYC_EXT.1/CMT Extended: Key chaining	FCS_KYC_EXT.1	[HCDcPP]	Yes	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)		[HCDcPP]	No	No	Yes	Yes
	FCS_SMC_EXT.1 Extended: Submask Combining		[HCDcPP]	No	No	No	Yes
FDP - User data protection	FDP_ACC.1 Subset access control		[HCDcPP]	No	No	No	No
	FDP_ACF.1 Security attribute based access control		[HCDcPP]	No	Yes	Yes	No
	FDP_DSK_EXT.1 Extended: Protection of Data on Disk		[HCDcPP]	No	No	No	Yes
FIA - Identification and authentication	FIA_AFL.1 Authentication failure handling		[HCDcPP]	No	No	Yes	Yes
	FIA_ATD.1 User attribute definition		[HCDcPP]	No	No	Yes	No
	FIA_PMG_EXT.1 Extended: Password Management		[HCDcPP]	No	No	Yes	Yes
	FIA_UAU.1 Timing of authentication		[HCDcPP]	No	No	Yes	No
	FIA_UAU.7 Protected authentication feedback		[HCDcPP]	No	No	Yes	No
	FIA_UID.1 Timing of identification		[HCDcPP]	No	No	Yes	No
	FIA_USB.1 User-subject binding		[HCDcPP]	No	No	Yes	No
	FIA_X509_EXT.1 Certificate Validation		[HCDcPP]	No	No	No	Yes
	FIA_X509_EXT.2 Certificate Authentication		[HCDcPP]	No	No	No	Yes
	FIA_X509_EXT.3 Certificate Requests		[HCDcPP]	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FMT - Security management	FMT_MOF.1 Management of security functions behaviour		[HCDcPP]	No	Yes	Yes	Yes
	FMT_MSA.1 Management of security attributes		[HCDcPP]	No	Yes	Yes	Yes
	FMT_MSA.3 Static attribute initialisation		[HCDcPP]	No	Yes	Yes	Yes
	FMT_MTD.1 Management of TSF data		[HCDcPP]	No	No	Yes	Yes
	FMT_SMF.1 Specification of Management Functions		[HCDcPP]	No	Yes	Yes	No
	FMT_SMR.1 Security roles		[HCDcPP]	No	No	No	No
FPT - Protection of the TSF	FPT_SBT_EXT.1 Secure Boot		[HCDcPP]	No	No	No	Yes
	FPT_KYP_EXT.1 Extended: Protection of Key and Material		[HCDcPP]	No	No	No	Yes
	FPT_SKP_EXT.1 Extended: Protection of TSF data		[HCDcPP]	No	No	No	No
	FPT_STM.1 Reliable time stamps		[HCDcPP]	No	No	No	No
	FPT_TST_EXT.1 Extended: TSF testing		[HCDcPP]	No	No	No	No
	FPT_TUD_EXT.1 Extended: Trusted Update		[HCDcPP]	No	No	No	Yes
FTA - TOE access	FTA_SSL.3 TSF-initiated termination		[HCDcPP]	No	No	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		[HCDcPP]	No	No	Yes	Yes
	FTP_TRP.1/Admin Trusted path (for Administrators)	FTP_TRP.1	[HCDcPP]	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FTP_TRP.1/NonAdmin Trusted path (for Non-administrators)	FTP_TRP.1	[HCDcPP]	No	No	No	Yes

6.1.1 Security audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

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 18**, **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 18**, **none**.

Table 18: Auditable events

Auditable event	Relevant SFR(s)	Additional information	Origin
Job completion	FDP_ACF.1	Type of job	[HCDcPP]
Unsuccessful login attempts limit is met or exceeded	FIA_AFL.1	Required by [HCDcPP]: • None Added by vendor: • User name associated with account	[HCDcPP]
Unsuccessful user authentication	FIA_UAU.1	Required by [HCDcPP]: • Supplied User ID/Name and origin of the attempt (e.g., IP address)	[HCDcPP]
Unsuccessful user identification	FIA_UID.1	Required by [HCDcPP]: • Supplied User ID/Name and origin of the attempt (e.g., IP address	[HCDcPP]

Auditable event	Relevant SFR(s)	Additional information	Origin
Use of management functions	FMT_SMF.1	Required by [HCDcPP]: • None	[HCDcPP]
Modification to the group of Users that are part of a role	FMT_SMR.1	Required by [HCDcPP]: • None	[HCDcPP]
Changes to the time	FPT_STM.1	Required by [HCDcPP]: • None Added by vendor: • New date and time • Old date and time	[HCDcPP]
Failure to establish session	FTP_ITC.1 FTP_TRP.1/Admin FTP_TRP.1/NonAdmin	Required by [HCDcPP]: • Reason for failure Added by vendor: • Non-TOE endpoint of connection (e.g., IP address)	[HCDcPP]
Unlocking an account	FIA_AFL.1	Required by [HCDcPP]: • None Added by vendor: • User name associated with account	Vendor
Unsuccessful attempt to validate a certificate	FIA_X509_EXT.1	Required by [HCDcPP]: • Reason for failure of certificate validation	[HCDcPP]

TSS Link: *TSS for FAU_GEN.1*.

6.1.1.2 FAU_GEN.2 User identity association

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 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide an Administrator with the capability to read all records from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

TSS Link: *TSS for FAU_SAR.1*.

6.1.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

TSS Link: *TSS for FAU_SAR.2*.

6.1.1.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

TSS Link: *TSS for FAU_STG.1*.

6.1.1.6 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records** and **no other actions** if the audit trail is full.

TSS Link: *TSS for FAU_STG.4*.

6.1.1.7 FAU_STG_EXT.1 Extended: External Audit Trail Storage

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 FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)

FCS_CKM.1.1/AKG The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- **RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;**
- **FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1**

- **FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526.**

TSS Link: *TSS for FCS_CKM.1/AKG*.

6.1.2.2 FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)

FCS_CKM.1.1/SKG The TSF shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes **256 bits** that meet the following: **NIST SP 800-133 Rev.2 Section 6.1, 6.3**.

TSS Link: *TSS for FCS_CKM.1/SKG*.

6.1.2.3 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526.**

TSS Link: *TSS for FCS_CKM.2*.

6.1.2.4 FCS_CKM_EXT.4 Extended: Cryptographic Key Material 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.

TSS Link: *TSS for FCS_CKM_EXT.4*.

6.1.2.5 FCS_CKM.4 Cryptographic key destruction

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

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

that meets the following: no standard.

TSS Link: *TSS for FCS_CKM.4*.

6.1.2.6 FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with specified cryptographic algorithms

- **AES used in CBC mode**

and cryptographic key sizes:

Case: AES algorithm

- **128 bits, 192 bits, 256 bits**

that meet the following:

Case: AES algorithm

- **ISO 18033-3, CBC as specified in ISO 10116**

TSS Link: *TSS for FCS_COP.1/DataEncryption*.

6.1.2.7 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm

- **RSA Digital Signature Algorithm and cryptographic key sizes (modulus) 2048 bits or 3072 bits**

that meet the following:
Case: RSA schemes

- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3**

TSS Link: *TSS for FCS_COP.1/SigGen*.

6.1.2.8 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm **SHA-256, SHA-384, SHA-512** and message digest sizes **160, 256, 384, 512** bits that meet the following: ISO/IEC 10118-3:2004**.**

TSS Link: *TSS for FCS_COP.1/Hash*.

6.1.2.9 FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)

FCS_COP.1.1/StorageEncryption The TSF shall perform data encryption and decryption in accordance with a specified cryptographic algorithm

- **AES used in CBC mode**

and cryptographic key sizes:
Case: AES algorithm

- **256 bits**

that meet the following:
Case: AES algorithm

- **ISO 18033-3, CBC as specified in ISO 10116**

TSS Link: *TSS for FCS_COP.1/StorageEncryption*.

6.1.2.10 FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)

FCS_COP.1.1/KeyEnc The TSF shall perform key encryption and decryption in accordance with a specified cryptographic algorithm
Case: AES algorithm

- **AES used in CBC mode and cryptographic key sizes 256 bits that meet the following: AES as specified in ISO/IEC 18033-3, CBC as specified in ISO/IEC 10116**

TSS Link: *TSS for FCS_COP.1/KeyEnc*.

6.1.2.11 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm **HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512** and cryptographic key sizes **160 bits, 256 bits, 384 bits, 512 bits** and message digest sizes **160, 256, 384, 512 bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

TSS Link: *TSS for FCS_COP.1/KeyedHash*.

6.1.2.12 FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication)

FCS_COP.1.1/CMAC The TSF shall perform cryptographic message authentication in accordance with a specified cryptographic algorithm **HMAC-SHA-256** and cryptographic key sizes **256 bits** used in **HMAC** that meet the following

- **ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”**

TSS Link: *TSS for FCS_COP.1/CMAC*.

6.1.2.13 FCS_IPSEC_EXT.1 Extended: IPsec selected

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 have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement **transport mode**.

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 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602)** together with a Secure Hash Algorithm (SHA)-based HMAC **HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512**.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol:

- **IKEv2 as defined in RFC 5996 and with no support for NAT traversal and RFC 4868 for hash functions.**

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the **IKEv2** protocol uses the cryptographic algorithms **AES-CBC-128, AES-CBC-192, AES-CBC-256 (specified in RFC 3602)**.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that

- **IKEv2 SA lifetimes can be configured by a Security Administrator based on:**
  - **length of time, where the time values can be configured within 1- 24 hours;**

FCS_IPSEC_EXT.1.8 The TSF shall ensure that

- **IKEv2 Child SA lifetimes can be configured by a Security Administrator based on:**
  - **length of time, where the time values can be configured within 1-8 hours;**

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least **256** bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in **IKEv2** exchanges of length

- **at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash**

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s)

- **14 (2048-bit MODP), 15 (3072-bit MODP) according to RFC 3526**

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the **IKEv2 IKE_SA** connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the **IKEv2 CHILD_SA** connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using **RSA** that use X.509v3 certificates that conform to RFC 4945 and **no other method**.

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: **SAN: IP address, SAN: Fully Qualified Domain Name (FQDN**, **Distinguished Name (DN)** and **SAN:email**.

TSS Link: *TSS for FCS_IPSEC_EXT.1*.

6.1.2.14 FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

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/CMAC, such that the output is at least of equivalent security strength (in number of bits) to the BEV or the DEK.

TSS Link: *TSS for FCS_KDF_EXT.1*.

6.1.2.15 FCS_KYC_EXT.1/CDE Extended: Key Chaining

FCS_KYC_EXT.1.1/CDE 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/KeyEnc** while maintaining an effective strength of **256 bits**.

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

6.1.2.16 FCS_KYC_EXT.1/CM Extended: Key Chaining

FCS_KYC_EXT.1.1/CM 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*.

6.1.2.17 FCS_KYC_EXT.1/CMT Extended: Key Chaining

FCS_KYC_EXT.1.1/CMT 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*.

6.1.2.18 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using **HMAC_DRBG (any), CTR_DRBG (AES)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **1 hardware based noise source** with a minimum of **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.

TSS Link: *TSS for FCS_RBG_EXT.1*.

6.1.2.19 FCS_SMC_EXT.1 Extended: Submask Combining

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

TSS Link: *TSS for FCS_SMC_EXT.1*.

6.1.3 User data protection (FDP)

6.1.3.1 FDP_ACC.1 Subset access control

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 19** and **Table 20**.

TSS Link: *TSS for FDP_ACC.1*.

6.1.3.2 FDP_ACF.1 Security attribute based access control

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 19** and **Table 20**.

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 19** and **Table 20**.

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 19: 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
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**	**allowed / denied**	**denied by design**	**allowed**
	U.NORMAL	**denied**	denied	denied by design	denied
	Unauthenticated	**allowed** (condition 1)	denied	denied by design	denied

Table 20: 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
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*.

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.

6.1.3.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall **perform encryption in accordance with FCS_COP.1/StorageEncryption**, such that any 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*.

6.1.4 Identification and authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure handling

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 FIA_ATD.1 User attribute definition

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 FIA_PMG_EXT.1 Extended: Password Management

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
  - **"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", """", "'", "`", "+", ",", "-", ".", "/", "\", ":", ";", "<", "=", ">", "?", "[", "]", "_", "|", "~", "{", "}";**
- 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 FIA_UAU.1 Timing of authentication

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*.

6.1.4.5 FIA_UAU.7 Protected authentication feedback

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*.

6.1.4.6 FIA_UID.1 Timing of identification

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 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 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*.

6.1.4.7 FIA_USB.1 User-subject binding

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 at the product control panel" 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*.

6.1.4.8 FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using **the Online Certificate Status Protocol (OCSP) as specified in RFC 6960**.
- The TSF shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

TSS Link: *TSS for FIA_X509_EXT.1*.

6.1.4.9 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **IPsec** and **no additional uses**.

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall **not accept the certificate**.

TSS Link: *TSS for FIA_X509_EXT.2*.

6.1.4.10FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and **Common Name, Organization, Organizational Unit, Country, State, Locality**.

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

TSS Link: *TSS for FIA_X509_EXT.3*.

6.1.5 Security management (FMT)

6.1.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform the actions defined in Table 21 on*** the functions **defined in Table 21** to U.ADMIN.

Table 21: 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 FIA_UAU.1 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.
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 the Device Administrator account must be enabled.
Enhanced security event logging	Enable, disable	FAU_GEN.1	In the evaluated configuration, enhanced security event logging must be enabled.
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 FMT_MSA.1 Management of security attributes

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 22 on** the security attributes **defined in Table 22** to **the authorized identified roles defined in Table 22**.

Table 22: 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
	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

TSS Link: *TSS for FMT_MSA.1*.

6.1.5.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the User Data Access Control SFP to provide **the properties defined in Table 22 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 22** to specify alternative initial values to override the default values when an object or information is created.

TSS Link: *TSS for FMT_MSA.3*.

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

6.1.5.4 FMT_MTD.1 Management of TSF data

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 23**.

Table 23: 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
Permission set associations (except on the Device Administrator account)	Add, delete, view	U.ADMIN	FDP_ACF.1 FMT_MSA.1
Permission set associations (only on the Device Administrator account)	View	U.ADMIN	
List of software, firmware, and related configuration data			
IPsec CA and identity certificates	Import, delete	U.ADMIN	FCS_IPSEC_EXT.1
IPsec policy	Change, view, add, delete	U.ADMIN	FCS_IPSEC_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 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **defined in Table 24**.

Table 24: Specification of management functions

Management function	SFR	TSS page number	Objectives
Management of Device Administrator password	FMT_MTD.1	137	O.USER_AUTHORIZATION, O.USER_I&A
Management of account lockout policy	FMT_MTD.1	137	O.USER_I&A
Management of minimum length password settings	FMT_MTD.1	137	
Management of Internal and External authentication mechanisms	FMT_MOF.1	135	
Management of "Allow users to choose alternate sign-in methods at the product control panel" function	FMT_MOF.1	135	
Management of session inactivity timeouts	FMT_MTD.1	137	
Management of permission set associations	FMT_MTD.1	137	O.ADMIN_ROLES
Management of permission set permissions	FMT_MSA.1	136	O.ACCESS_CONTROL
Management of CA and identity certificates for IPsec authentication	FMT_MTD.1	137	O.COMMS_PROTECTION
Management of IPsec policy	FMT_MTD.1	137	O.COMMS_PROTECTION
Management of enhanced security event logging	FMT_MOF.1	135	O.AUDIT
Management of NTS configuration data	FMT_MTD.1	137	

TSS Link: *TSS for FMT_SMF.1*.

6.1.5.6 FMT_SMR.1 Security roles

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 FPT_SBT_EXT.1 Extended: Secure Boot

FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in an immutable Root of Trust.

FPT_SBT_EXT.1.2 At boot time the TSF shall use the chain(s) of trust to confirm integrity of its firmware/software using a **digital signature** verification method.

FPT_SBT_EXT.1.3 The TSF shall **reboot the device, halt boot process** in the event of a boot time verification failure so that the corrupted firmware/software isn't executed.

FPT_SBT_EXT.1.4 Following failure of verification, the TSF shall provide a mechanism to: **reinstall TOE image**.

FPT_SBT_EXT.1.5 The TSF shall contain **hash data** in the Hardware Root of Trust.

FPT_SBT_EXT.1.6 The TSF shall make the symmetric key accessible only to the Hardware Root of Trust.

TSS Link: *TSS for FPT_SBT_EXT.1*.

6.1.6.2 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall:

- **only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1/KeyWrap, or encrypted, as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport, encrypted or wrapped within a protected storage device using a key stored within that device,**
- **only store plaintext keys that meet any one of the following criteria:**
  - **the non-volatile memory where the key is stored on is located in a protected storage device**

TSS Link: *TSS for FPT_KYP_EXT.1*.

6.1.6.3 FPT_SKP_EXT.1 Extended: Protection of TSF Data

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*.

HCDcPP 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.

6.1.6.4 FPT_STM.1 Reliable time stamps

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

TSS Link: *TSS for FPT_STM.1*.

6.1.6.5 FPT_TST_EXT.1 Extended: TSF testing

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*.

6.1.6.6 FPT_TUD_EXT.1 Extended: Trusted Update

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 **digital signature** 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 FTA_SSL.3 TSF-initiated termination

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 FTP_ITC.1 Inter-TSF trusted channel

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: remote audit server, **authentication server, DNS server, NTS server, SMB server, SMTP 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 remote audit **server, authentication server, DNS server, NTS server, SMB server, SMTP server, and WINS server**.

TSS Link: *TSS for FTP_ITC.1*.

6.1.8.2 FTP_TRP.1/Admin Trusted path (for Administrators)

FTP_TRP.1.1/Admin 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/Admin The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin 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/Admin*.

6.1.8.3 FTP_TRP.1/NonAdmin Trusted path (for Non-administrators)

FTP_TRP.1.1/NonAdmin 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/NonAdmin The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/NonAdmin 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/NonAdmin*.

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 25: Mapping of security functional requirements to security objectives

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FAU_SAR.1	O.AUDIT
FAU_SAR.2	O.AUDIT
FAU_STG.1	O.AUDIT
FAU_STG.4	O.AUDIT
FAU_STG_EXT.1	O.AUDIT

Security functional requirements	Objectives
FCS_CKM.1/AKG	O.COMMS_PROTECTION O.STRONG_CRYPTO
FCS_CKM.1/SKG	O.COMMS_PROTECTION O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_CKM.2	O.COMMS_PROTECTION O.STRONG_CRYPTO
FCS_CKM.4	O.COMMS_PROTECTION O.STORAGE_ENCRYPTION
FCS_CKM_EXT.4	O.COMMS_PROTECTION O.STORAGE_ENCRYPTION
FCS_COP.1/CMAC	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_COP.1/DataEncryption	O.COMMS_PROTECTION O.STRONG_CRYPTO
FCS_COP.1/Hash	O.COMMS_PROTECTION O.STORAGE_ENCRYPTION O.UPDATE_VERIFICATION O.STRONG_CRYPTO
FCS_COP.1/KeyedHash	O.COMMS_PROTECTION O.STRONG_CRYPTO
FCS_COP.1/KeyEnc	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_COP.1/SigGen	O.COMMS_PROTECTION O.UPDATE_VERIFICATION O.STRONG_CRYPTO
FCS_COP.1/StorageEncryption	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_IPSEC_EXT.1	O.COMMS_PROTECTION O.STRONG_CRYPTO
FCS_KDF_EXT.1	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_KYC_EXT.1/CDE	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO

Security functional requirements	Objectives
FCS_KYC_EXT.1/CM	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_KYC_EXT.1/CMT	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_RBG_EXT.1	O.COMMS_PROTECTION O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FCS_SMC_EXT.1	O.STORAGE_ENCRYPTION O.STRONG_CRYPTO
FDP_ACC.1	O.ACCESS_CONTROL O.USER_AUTHORIZATION
FDP_ACF.1	O.ACCESS_CONTROL O.USER_AUTHORIZATION
FDP_DSK_EXT.1	O.STORAGE_ENCRYPTION
FIA_AFL.1	O.USER_I&A O.AUTH_FAILURES
FIA_ATD.1	O.USER_AUTHORIZATION
FIA_PMG_EXT.1	O.USER_I&A
FIA_UAU.1	O.USER_I&A
FIA_UAU.7	O.USER_I&A
FIA_UID.1	O.ADMIN_ROLES, O.USER_I&A
FIA_USB.1	O.USER_I&A
FIA_X509_EXT.1	O.COMMS_PROTECTION
FIA_X509_EXT.2	O.COMMS_PROTECTION
FIA_X509_EXT.3	O.COMMS_PROTECTION
FMT_MOF.1	O.ADMIN_ROLES
FMT_MSA.1	O.ACCESS_CONTROL, O.USER_AUTHORIZATION
FMT_MSA.3	O.ACCESS_CONTROL, O.USER_AUTHORIZATION

Security functional requirements	Objectives
FMT_MTD.1	O.ACCESS_CONTROL
FMT_SMF.1	O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION, O.COMMS_PROTECTION
FMT_SMR.1	O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION
FPT_SBT_EXT.1	O.FW_INTEGRITY
FPT_KYP_EXT.1	O.KEY_MATERIAL O.STRONG_CRYPTO
FPT_SKP_EXT.1	O.COMMS_PROTECTION
FPT_STM.1	O.AUDIT O.STRONG_CRYPTO
FPT_TST_EXT.1	O.TSF_SELF_TEST
FPT_TUD_EXT.1	O.UPDATE_VERIFICATION
FTA_SSL.3	O.USER_I&A
FTP_ITC.1	O.AUDIT O.COMMS_PROTECTION
FTP_TRP.1/Admin	O.COMMS_PROTECTION
FTP_TRP.1/NonAdmin	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 26: Security objectives for the TOE rationale

Security objectives	SFR	Relationship	Rationale
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.

Security objectives	SFR	Relationship	Rationale
	FIA_ATD.1	Supports	This SFR defines the attributes that are associated with Users that can be used to define their authorizations.
	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.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

Security objectives	SFR	Relationship	Rationale
			that govern their authorizations to the TSF upon successful authentication to the TOE.
	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.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

Security objectives	SFR	Relationship	Rationale
			purposes of determining authentication and authorization.
O.UPDATE_VERIFICATION	FCS_COP.1/SigGen	Selection	This SFR defines the digital signature service(s) used to verify the authenticity TOE updates.
	FCS_COP.1/Hash	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.
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/AKG	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/SKG	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/DataEncryption	Satisfies	This SFR defines the use of a secure symmetric key algorithm that is used for protected communications.
	FCS_COP.1/SigGen	Satisfies	This SFR defines the digital signature services(s) used for protected communications.
	FCS_COP.1/Hash	Selection	This SFR defines the hashing algorithm(s) used during IKE/IPsec.

Security objectives	SFR	Relationship	Rationale
	FCS_COP.1/KeyedHash	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 allows cryptographic functions to operate with their theoretical maximum strengths.
	FIA_X509_EXT.1	Supports	This SFR supports protected communications by defining the rules for the validation of X.509 certificates used in IPsec.
	FIA_X509_EXT.2	Supports	This SFR supports protected communications by defining the use of X.509 certificates for authentication of the protocols used for secure transmission of user and TSF data between the TOE and a trusted external IT entity.
	FIA_X509_EXT.3	Supports	This SFR supports protected communications by defining the rules for a certificate request for an X.509 certificate which is used in IPsec.
	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/Admin	Satisfies	This SFR defines the protected communications path that is used to secure Administrator interaction with the TOE.

Security objectives	SFR	Relationship	Rationale
	FTP_TRP.1/NonAdmin	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_SAR.1	Supports	This SFR defines the ability of the TOE to provide the Administrator with the capability to read all records from the audit records and in a suitable manner for the user to interpret the information.
	FAU_SAR.2	Supports	This SFR defines that the TSF shall restrict users read access to the audit records, except users who have been granted explicit read-access.
	FAU_STG.1	Supports	This SFR defines that the TSF shall protect the stored audit records from unauthorized deletion and modification.
	FAU_STG.4	Supports	This SFR defines what actions the TSF shall take when the audit trail is full.
	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.
O.STORAGE_ENCRYPTION	FCS_CKM.1/SKG	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

Security objectives	SFR	Relationship	Rationale
			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/Hash	Supports	This SFR defines the hashing services used by the TOE when deriving the key-slot key for customer data encryption.
	FCS_COP.1/DataEncryption	Supports	This SFR defines the cryptographic algorithms that must be applied to encrypt/decrypt data that is to be transmitted to/from the TOE.
	FCS_COP.1/StorageEncryption	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/KeyEnc	Supports	This SFR defines the encryption/decryption algorithms used by the TOE to encrypt/decrypt the master key used for storage encryption.
	FCS_COP.1/CMAC	Option	This SFR defines the keyed-hash message authentication used by the TOE when deriving the key-slot key 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-slot key used for customer data encryption.
	FCS_KYC_EXT.1/CDE	Satisfies	This SFR defines the key chaining method used by the TOE for customer 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

Security objectives	SFR	Relationship	Rationale
			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_RBG_EXT.1	Supports	This SFR defines the random bit generation algorithm used to ensure that the TOE's cryptographic algorithms function with the theoretical maximum level of security.
	FCS_SMC_EXT.1	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.AUTH_FAILURES	FIA_AFL.1	Satisfies	This SFR defines how many consecutive unsuccessful authentication failures to prove a user's identity trigger actions by the TOE and what those actions will be.
O.FW_INTEGRITY	FPT_SBT_EXT.1	Satisfies	This SFR defines how the integrity of firmware/software at boot time is to be verified via chains of trust, each one anchored in its own root of trust.
	FCS_COP.1/Hash	Supports	This SFR ensures the use of strong hash mechanisms.
O.STRONG_CRYPTO	FCS_CKM.1/SKG	Satisfies	This SFR ensures the generation of strong symmetric keys.
	FCS_CKM.2	Satisfies	This SFR ensures the use of strong key establishment mechanisms.
	FCS_COP.1/DataEncryption	Satisfies	This SFR ensures the use of strong methods to perform data encryption/decryption for protected communications.

Security objectives	SFR	Relationship	Rationale
	FCS_COP.1/SigGen	Satisfies	This SFR ensures the use of strong digital signature services.
	FCS_COP.1/Hash	Satisfies	This SFR ensures the use of strong hash mechanisms.
	FCS_RBG_EXT.1	Satisfies	This SFR ensures the use of strong random bit generation mechanisms.
	FPT_STM.1	Supports	This SFR provides reliable system time services that may be used as inputs to cryptographic functions.
	FCS_COP.1/StorageEncryption	Satisfies	This SFR ensures the use of strong methods to perform data encryption/decryption.
	FCS_COP.1/KeyEnc	Satisfies	This SFR ensures the use of strong methods to perform key encryption.
	FCS_SMC_EXT.1	Satisfies	This SFR ensures the use of strong methods to perform submask combining.
	FCS_IPSEC_EXT.1	Satisfies	This requirement defines the implementation of IPsec using strong cryptography.
	FCS_COP.1/KeyedHash	Satisfies	This SFR ensures the use of strong methods to perform keyed-hash message authentication.
	FCS_KDF_EXT.1	Satisfies	This SFR ensures the use of strong methods for performing cryptographic key derivation.
	FCS_COP.1/CMAC	Satisfies	This SFR ensures the use of strong methods to perform message authentication.
	FCS_CKM.1/AKG	Satisfies	This SFR ensures the generation of strong asymmetric keys.
	FPT_KYP_EXT.1	Satisfies	This SFR ensures the use of strong methods to protection of key and key material.
	FCS_KYC_EXT.1/CDE	Satisfies	This SFR defines the key chaining method used by the TOE for customer data encryption to provide multiple layers of security for key material.

Security objectives	SFR	Relationship	Rationale
	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.

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of the SFRs modeled in [HCDcPP] and how the SFRs for the TOE resolve those dependencies.

Table 27: TOE SFR dependency analysis

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
	FTP_ITC.1	FTP_ITC.1
FCS_CKM.1/AKG	FCS_CKM.2 or FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_CKM.1/SKG	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/StorageEncryption	FCS_COP.1/StorageEncryption
	FCS_COP.1/KeyWrap	This dependency is unresolved as the TSF does not support key wrapping.
	FCS_COP.1/KeyEnc	FCS_COP.1/KeyEnc

Security functional requirement	Dependencies	Resolution
	FCS_COP.1/KeyedHash	The dependency remains unresolved, as symmetric key generation has no dependency on a keyed hash.
	FCS_COP.1/CMAC	This dependency remains unresolved, as symmetric key generation is not dependent on cipher-based message authentication.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_CKM.2	FCS_CKM.1/AKG	FCS_CKM.1/AKG
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_CKM_EXT.4	FCS_CKM.1/AKG or FCS_CKM.1/SKG	FCS_CKM.1/AKG FCS_CKM.1/SKG
	FCS_CKM.2	FCS_CKM.2
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	FCS_CKM.1/AKG or FCS_CKM.1/SKG	FCS_CKM.1/AKG FCS_CKM.1/SKG
FCS_COP.1/DataEncryption	FCS_CKM.1/SKG	FCS_CKM.1/SKG
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_COP.1/SigGen	FCS_CKM.1/AKG	FCS_CKM.1/AKG
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_COP.1/Hash	None	n/a
FCS_RBG_EXT.1	None	n/a
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3
FIA_ATD.1	None	n/a
FIA_PMG_EXT.1	None	n/a

Security functional requirement	Dependencies	Resolution
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	None	n/a
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	FDP_ACC.1, or ~~FDP_IFC.1~~	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_SBT_EXT.1	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/KeyedHash	This dependency is unresolved because the TOE’s secure boot functionality does not utilize a keyed hash algorithm.
	FCS_COP.1/DataEncryption	This dependency is unresolved because the TOE’s secure boot functionality does not utilize a data encryption algorithm.
	FCS_COP.1/StorageEncryption	This dependency is unresolved because the TOE’s secure boot functionality does not utilize a data encryption algorithm.

Security functional requirement	Dependencies	Resolution
	FCS_COP.1/CMAC	The dependency is unresolved, as the TOE's secure boot mechanism does not utilize a cipher-based message authentication function.
FPT_SKP_EXT.1	None	n/a
FPT_STM.1	None	n/a
FPT_TST_EXT.1	None	n/a
FPT_TUD_EXT.1	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
FTA_SSL.3	None	n/a
FTP_ITC.1	FCS_IPSEC_EXT.1, or FCS_TLSC_EXT and/or FCS_TLSS_EXT, or FCS_SSHC_EXT or FCS_SSHS_EXT, or FCS_DTLSC_EXT and/or FCS_DTLSS_EXT, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1
FTP_TRP.1/Admin	FCS_IPSEC_EXT.1, or FCS_TLSC_EXT and/or FCS_TLSS_EXT, or FCS_SSHC_EXT or FCS_SSHS_EXT, or FCS_DTLSC_EXT and/or FCS_DTLSS_EXT, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1
FCS_COP.1/StorageEncryption	FCS_CKM.1/SKG, or ~~FDP_IFC.1~~	FCS_CKM.1/SKG
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_COP.1/KeyEnc	FCS_CKM.1/SKG, or ~~FDP_IFC.1~~	FCS_CKM.1/SKG
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_SMC_EXT.1	FCS_COP.1/Hash	This dependency is unresolved, as the TSF does not use a hash function to combine submasks for key generation.

Security functional requirement	Dependencies	Resolution
FCS_IPSEC_EXT.1	~~FPT_ITT.1~~	n/a
	FIA_PSK_EXT.1	The dependency is unresolved, as the TOE’s IPsec functionality does not support pre-shared keys for peer authentication in the evaluated configuration.
	FCS_CKM.1/AKG	FCS_CKM.1/AKG
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_COP.1/KeyedHash	FCS_RBG_EXT.1	FCS_RBG_EXT.1
	FTP_ITC.1 or FCS_CKM.1/AKG	FTP_ITC.1 FCS_CKM.1/AKG
	FCS_CKM.4	FCS_CKM.4
FCS_KDF_EXT.1	FCS_COP.1/CMAC	FCS_COP.1/CMAC
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	if selected FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_COP.1/CMAC	~~FDP_ITC.1, or~~ ~~FDP_ITC.2, or~~ FCS_CKM.1/SKG	FCS_CKM.1/SKG
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FIA_X509_EXT.1	FCS_X509_EXT.2	FIA_X509_EXT.2
FIA_X509_EXT.2	FCS_CKM.1/AKG	FCS_CKM.1/AKG
	FCS_CKM.1/SKG	The dependency is unresolved, as the TOE’s IPsec functionality does not rely on symmetric key authentication when using X.509 certificates for peer authentication.

Security functional requirement	Dependencies	Resolution
	FIA_X509_EXT.1	FIA_X509_EXT.1
FIA_X509_EXT.3	FCS_CKM.1/AKG	FCS_CKM.1/AKG
	FIA_X509_EXT.1	FIA_X509_EXT.1
FPT_KYP_EXT.1	FCS_KYC_EXT.1	FCS_KYC_EXT.1/CDE FCS_KYC_EXT.1/CM FCS_KYC_EXT.1/CMT
FCS_KYC_EXT.1/CDE	FCS_COP.1/KeyWrap	The dependency is unresolved, as the TSF does not wrap any of the keys in the key chain for customer data encryption.
	FCS_SMC_EXT.1	The dependency is unresolved, as the TSF does not combine submasks to generate any keys in the key chain for customer data encryption.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	FCS_COP.1/KeyEnc	FCS_COP.1/KeyEnc
	FCS_KDF_EXT.1, and/or	FCS_KDF_EXT.1
	FCS_COP.1/KeyTransport	The dependency is unresolved, as the TSF does not use key transport to generate any keys in the key chain for customer data encryption.
FCS_KYC_EXT.1/CM	FCS_COP.1/KeyWrap	The dependency is unresolved, as the TSF does not wrap any of the keys in the key chain for encrypting the certificates XML file.
	FCS_SMC_EXT.1	The dependency is unresolved, as the TSF does not combine submasks to generate any keys in the key chain for encrypting the certificates XML file.
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	FCS_COP.1/KeyEnc	The dependency is unresolved, as the TSF does not encrypt any keys in the key chain for encrypting the certificates XML file.

Security functional requirement	Dependencies	Resolution
	FCS_KDF_EXT.1, and/or	The dependency is unresolved, as the TSF does not perform key derivation to generate any keys in the key chain used for encrypting the certificates XML file.
	FCS_COP.1/KeyTransport	The dependency is unresolved, as the TSF does not use key transport to generate any keys in the key chain for encrypting the certificates XML file.
FCS_KYC_EXT.1/CMT	FCS_COP.1/KeyWrap	The dependency is unresolved, as the TSF does not wrap any of the keys in the key chain used to encrypt identity certificates and their corresponding private keys, which are stored in individual files (a.k.a., thumbprint files).
	FCS_SMC_EXT.1	FCS_SMC_EXT.1
	FCS_CKM_EXT.4	FCS_CKM_EXT.4
	FCS_COP.1/KeyEnc	The dependency is unresolved, as the TSF does not encrypt any keys in the key chain to encrypt identity certificates and their corresponding private keys, which are stored in individual files (a.k.a., thumbprint files).
	FCS_KDF_EXT.1, and/or	The dependency is unresolved, as the TSF does not perform key derivation to generate any keys in the key chain used to encrypt identity certificates and their corresponding private keys, which are stored in individual files (a.k.a., thumbprint files).

Security functional requirement	Dependencies	Resolution
	FCS_COP.1/KeyTransport	The dependency is unresolved, as the TSF does not use key transport to generate any keys in the key chain used to encrypt identity certificates and their corresponding private keys, which are stored in individual files (a.k.a., thumbprint files).
FDP_DSK_EXT.1	FCS_COP.1/StorageEncryption	FCS_COP.1/StorageEncryption
FTP_TRP.1/NonAdmin	FCS_IPSEC_EXT.1, or FCS_TLSC_EXT and/or FCS_TLSS_EXT, or FCS_SSHC_EXT or FCS_SSHS_EXT, or FCS_DTLSC_EXT and/or FCS_DTLSS_EXT, or FCS_HTTPS_EXT.1	FCS_IPSEC_EXT.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1

6.2.4 HCDcPP SFR reconciliation

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

Table 28: HCD cPP SFRs excluded from the ST

Excluded PP SFR	Type	Rationale
FCS_COP.1/KeyWrap	Selection-based	FCS_COP.1/KeyWrap is defined in [HCDcPP] 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/CDE, FCS_KYC_EXT.1/CM, or FCS_KYC_EXT.1/CMT.
FCS_COP.1/KeyTransport	Selection-based	FCS_COP.1/KeyTransport is defined in [HCDcPP] 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/CDE, FCS_KYC_EXT.1/CM, or FCS_KYC_EXT.1/CMT.
FCS_TLSC_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_TLSS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.

Excluded PP SFR	Type	Rationale
FCS_TLSC_EXT.2	Optional	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_TLSS_EXT.2	Optional	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_SSHC_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_SSHS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_HTTPS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_DTLSC_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_DTLSS_EXT.1	Selection-based	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_DTLSC_EXT.2	Optional	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FCS_DTLSS_EXT.2	Optional	All communication channels are protected by IPsec. See FCS_IPSEC_EXT.1 for more information.
FIA_PSK_EXT.1	Selection-based	FCS_IPSEC_EXT.1.13 requires the use of X.509v3 certificates to perform peer authentication for IPsec and optionally allows the selection of Pre-shared Keys. In the evaluated configuration, no other method can be used in addition to X.509v3 certificates for peer authentication for IPsec.
FCS_PCC_EXT.1	Selection-based	FCS_PCC_EXT.1 is defined in [HCDcPP] for cryptographic password construction and conditioning of the BEV. The TOE does not support the manual entry of a passphrase to generate a password authorization factor.
FCS_SNI_EXT.1	Selection-based	FCS_SNI_EXT.1 is defined in [HCDcPP] 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.
FDP_FXS_EXT.1	Conditionally Mandatory	FDP_FXS_EXT.1 is defined in [HCDcPP] for prohibiting communication via the fax interface, except transmitting or receiving User Data using fax protocols. Fax functionality is not supported by the TOE.

Excluded PP SFR	Type	Rationale
FDP_UDU_EXT.1	Optional	FDP_UDU_EXT.1 is defined in [HCDcPP] for requiring the TSF to make User Document Data stored on wear-leveling and non-wear-leveling storage devices unavailable via either overwrite or destruction of cryptographic keys to ensure that this data does not remain on the device in the TOE after a Document Processing job has been completed or cancelled. This requirement is optional.
FPT_WIPE_EXT.1	Optional	FPT_WIPE_EXT.1 is defined in [HCDcPP] for ensuring that any previous customer-supplied information content of a resource in non-volatile storage is made unavailable upon the request of an Administrator. This requirement is optional.

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 29: Security assurance requirements

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
Security Target (ASE)	Conformance Claims (ASE_CCL.1)	CC Part 3	No	No	No	No
	Extended components definition (ASE_ECD.1)	CC Part 3	No	No	No	No
	ST introduction (ASE_INT.1)	CC Part 3	No	No	No	No
	Security objectives for the operational environment (ASE_OBJ.1)	CC Part 3	No	No	No	No
	Stated security requirements (ASE_REQ.1)	CC Part 3	No	No	No	No
	Security Problem Definition (ASE_SPD.1)	CC Part 3	No	No	No	No
	TOE summary specification (ASE_TSS.1)	CC Part 3	No	No	No	No
Development (ADV)	Basic functional specification (ADV_FSP.1)	CC Part 3	No	No	No	No
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)	CC Part 3	No	No	No	No
	Preparative procedures (AGD_PRE.1)	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.1)	CC Part 3	No	No	No	No
	TOE CM coverage (ALC_CMS.1)	CC Part 3	No	No	No	No
Tests (ATE)	Independent testing – conformance (ATE_IND.1)	CC Part 3	No	No	No	No
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)	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 30 provide a quick index to each SFR's TSS entry in Table 31 of the next section.

Table 30: TSS index

SFR	TSS page	SFR	TSS page	SFR	TSS page	SFR	TSS page
FAU_GEN.1	101	FCS_COP.1/Hash	114	FDP_DSK_EXT.1	125	FMT_MTD.1	137
FAU_GEN.2	106	FCS_COP.1/Storage Encryption	116	FIA_AFL.1	126	FMT_SMF.1	139
FAU_SAR.1	106	FCS_COP.1/KeyEnc	117	FIA_ATD.1	127	FMT_SMR.1	140
FAU_SAR.2	106	FCS_COP.1/KeyedHash	117	FIA_PMG_EXT.1	128	FPT_SBT_EXT.1	141
FAU_STG.1	106	FCS_COP.1/CMAC	118	FIA_UAU.1	128	FPT_KYP_EXT.1	141
FAU_STG.4	107	FCS_IPSEC_EXT.1	118	FIA_UAU.7	130	FPT_SKP_EXT.1	141
FAU_STG_EXT.1	107	FCS_KDF_EXT.1	121	FIA_UID.1	131	FPT_STM.1	142
FCS_CKM.1/AKG	107	FCS_KYC_EXT.1/CDE	121	FIA_USB.1	131	FPT_TST_EXT.1	142
FCS_CKM.1/SKG	108	FCS_KYC_EXT.1/CM	122	FIA_X509_EXT.1	134	FPT_TUD_EXT.1	142
FCS_CKM.2	109	FCS_KYC_EXT.1/CMT	122	FIA_X509_EXT.2	134	FTA_SSL.3	143
FCS_CKM_EXT.4	109	FCS_RBG_EXT.1	123	FIA_X509_EXT.3	134	FTP_ITC.1	143
FCS_CKM.4	110	FCS_SMC_EXT.1	123	FMT_MOF.1	135	FTP_TRP.1/Admin	144
FCS_COP.1/DataEncryption	113	FDP_ACC.1	124	FMT_MSA.1	136	FTP_TRP.1/NonAdmin	144
FCS_COP.1/SigGen	113	FDP_ACF.1	124	FMT_MSA.3	137		

7.1.1 TOE SFR compliance rationale

Table 31 provides the rationale for how the TOE complies with each of the SFRs in Section 6.1.

Table 31: TOE SFR compliance rationale

TOE SFRs and compliance rationale
FAU_GEN.1 (Audit generation)
Objective(s): O.AUDIT

TOE SFRs and compliance rationale

Summary: The TOE generates audit records for the audit events specified in [HCDcPP]. 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 32 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 32: TOE audit records

Auditable event	**Additional information**	**CCECG "*Syslog messages*" category and records**
Start-up and shutdown of the audit functions	None	Enhanced security event logging: • Auditing was started during boot up • Auditing was stopped using EWS • Auditing was restarted using EWS
Job completion	Type of job	Job completion: • Save to Device Memory job completion • Retrieve from Device Memory job completion (Print from job storage) • Print job completion
Unsuccessful login attempts limit is met or exceeded	Required by [HCDcPP]: • None Added by vendor: • User name associated with account	Account entered lockout (protected) mode: • Account Entered Lockout Mode
Unsuccessful user authentication	Required by [HCDcPP]: • Supplied User ID/Name and origin	Local device sign in: • Local Device sign-in method failed
		Windows sign in:

TOE SFRs and compliance rationale

	of the attempt (e.g., IP address)	- Windows sign-in method failed for the specified user
		LDAP sign in: - LDAP sign-in method failed for the specified user
Unsuccessful user identification	Required by [HCDcPP]: - Supplied User ID/Name and origin of the attempt (e.g., IP address)	Same categories and records as the "Unsuccessful user authentication" auditable events
Use of the management functions	Required by [HCDcPP]: None	Device administrator password: - Device Administrator Password modified
		Account lockout policy: - Account Lockout Policy enabled - Account Lockout Policy disabled - Account Lockout Policy setting modified
		Minimum password length settings: - Minimum Password Length Policy setting modified
		Windows Sign In: - Windows Sign In enabled - Windows Sign In disabled - Windows Sign In configuration modified
		LDAP Sign In: - LDAP Sign In enabled - LDAP Sign In disabled - LDAP Sign In configuration modified

TOE SFRs and compliance rationale		
		"Allow users to choose alternate sign-in methods at the product control panel" function: • Sign In and Permission Policy settings modified
		Session inactivity timeout: • Control Panel Inactivity Timeout Changed • EWS Session Timeout modified
		Permission set associations: • Default Permission set for sign-in method modified • User to Permission Set Relationship added • User to Permission Set Relationship deleted • Group to Permission Set Relationship added • Group to Permission Set Relationship deleted
		Custom permission sets: • Permission Set added • Permission Set modified • Permission Set copied • Permission Set deleted
		Permissions associated with permission sets: • Permission Set modified
		IPsec policies: • IPsec policy added • IPsec policy modified • IPsec policy deleted
		CA and identity certificates used for IPsec authentication: • Device CA certificate installed • Device CA certificate deleted • Device Identity certificate and private key installed • Certificate selected for IPSec usage • Device Identity certificate deleted

TOE SFRs and compliance rationale

		Enhanced security event logging: • CCC logging started • CCC logging stopped
		NTS configuration data: • Date and Time configuration modified
Modifications to the group of users that are part of a role	Required by [HCDcPP]: • None	Network user to permission set relationships: • User to Permission Set Relationship added • User to Permission Set Relationship deleted
		Network group to permission set relationships: • Group to Permission Set Relationship added • Group to Permission Set Relationship deleted
Changes to the time	Required by [HCDcPP]: • None Added by vendor: • New date and time • Old date and time	System time: • System time changed
Failure to establish session (trusted channel/path)	Required by [HCDcPP]: • Reason for failure Added by vendor: • Non-TOE endpoint of connection (e.g., IP address)	IKEv2 phase 1 negotiations: • IKEv2 phase 1 negotiation failed initiated by the client computer • IKEv2 phase 1 negotiation failed initiated by the local device (TOE)
		IKEv2 phase 2 negotiations: • IKEv2 phase 2 negotiation failed initiated by the client computer • IKEv2 phase 2 negotiation failed initiated by the local device (TOE)
Unlocking an account	Required by [HCDcPP]: • None Added by vendor: • User name associated with account	Account exited lockout (protected) mode: • Account Exited Lockout Mode

TOE SFRs and compliance rationale

Unsuccessful attempt to validate a certificate	Required by [HCDcPP]: • Reason for failure of certificate validation	Attempt to perform an OCSP certificate revocation check and IKEv2 phase 1 negotiations: • OCSP certificate revocation check • IKEv2 phase 1 negotiation failed initiated by the client computer • IKEv2 phase 1 negotiation failed initiated by the local device (TOE)

FAU_GEN.2 (Audit user identification)

Objective(s): O.AUDIT

Summary: Events resulting from actions of identified users are associated with the identity of the user that caused the event.

FAU_SAR.1 (Audit review)

Objective(s): O.AUDIT

Summary: An audit record is created, placed into a queue, immediately transmitted from the queue to the syslog server, and written to the internal log file. Once the syslog server successfully receives the record, it is removed from the queue.

The TOE retains up to 2500 audit records in an internal log file on the storage device, replacing the oldest records with new ones when the log file reaches its capacity. These audit records can be exported via the EWS interface. Access to the export function is limited to U.ADMIN. For addition information on user identification and authentication through the EWS interface, see EWS I&A.

The exported audit records are stored in a JSON file, with each record enclosed in curly braces (“{}”) and separated by a comma (“,”).

FAU_SAR.2 (Restricted audit review)

Objective(s): O.AUDIT

Summary: The TOE connects to an external syslog server to send audit records for long-term storage and review. It uses the syslog protocol to transmit these records over an IPsec channel, which ensures data protection and verifies the identities of both endpoints.

Additionally, the TOE stores up to 2500 audit records in an internal log file on the storage device, overwriting the oldest records with new ones when the file reaches its capacity. These records can be exported through the EWS interface, with access to the export function restricted to U.ADMIN. For more information on user identification and authentication via the EWS interface, refer to EWS I&A.

FAU_STG.1 (Protected audit trail storage)

Objective(s): O.AUDIT

TOE SFRs and compliance rationale
Summary: The TOE stores up to 2500 audit records in an internal log file on the storage device. These records can be exported through the EWS interface, with access to the export function restricted to U.ADMIN. The only action allowed on these audit records is exporting; they cannot be modified or deleted by any TOE user.
FAU_STG.4 (Prevention of audit data loss)
Objective(s): O.AUDIT **Summary**: See the TSS for FAU_STG_EXT.1.
FAU_STG_EXT.1 (Audit trail storage)
Objective(s): O.AUDIT **Summary**: The TOE connects and sends audit records to an external syslog server for long-term storage and audit review. It uses the syslog protocol to transmit the records over an IPsec channel. The IPsec channel provides protection of the transmitted data and assured identification of both endpoints. The TOE contains two in-memory audit record message queues. One queue is for network audit records (e.g., IKEv2 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. The network queue holds up to 15 audit records. New audit records are discarded when the network queue becomes full. The HCD queue holds up to 1000 audit records. New audit records replace the oldest audit records when the HCD queue becomes full. The TOE establishes a persistent connection to the external syslog server. An audit record is generated, added to a queue, immediately sent from the queue to the syslog server and written to the internal log file, then removed from the queue once the record has been successfully received by the syslog server. If the connection is interrupted (e.g., network outage), the TOE will make 5 attempts to reestablish the connection where each attempt lasts for approximately 30 seconds. If all attempts fail, the TOE will repeat the reestablishment process again when a new audit record is added to the HCD queue. Once the connection is reestablished, the records from both queues are immediately sent to the syslog server. If the TOE is powered off, any audit records remaining in the two in-memory messages queues at the time of power-off will be discarded. The TOE also stores up to 2500 audit records in an internal log file on the storage device 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.
FCS_CKM.1/AKG (Asymmetric key generation)
Objective(s): O.COMMS_PROTECTION, O.STRONG_CRYPTO **Summary**: For IPsec IKEv2 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

TOE SFRs and compliance rationale

generation algorithm. Because of this, the cryptographic algorithm testing for DH contains a prerequisite for testing the DSA key generation function used by the DH key generation function. Thus, DSA key generation is a prerequisite for and included as part of KAS FFC.

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

- L=2048, N=224
- L=2048, N=256
- L=3072, N=256

For KAS FFC, any necessary key material is obtained using the QuickSec 9.1 Cryptographic Module CTR_DRBG (AES) defined in FCS_RBG_EXT.1.

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 IKEv2 KDF.

The TOE uses RSA-based X.509v3 certificates for IKEv2/IPsec authentication using the IPsec IKEv2 digital signature authentication method. (See FCS_COP.1/SigGen for RSA digital signature generation and verification.)

The TOE provides the administrator with the capability to generate an RSA certificate signing request. During this process, the TOE generates an RSA public/private key pair using the HP FutureSmart Firmware OpenSSL 1.1.1 CTR_DRBG (AES) random bit generator, as specified in FCS_RBG_EXT.1. The RSA key pair generation supports the following key sizes:

- 2084 bits
- 3072 bits

Table 33: Asymmetric key generation

Usage	Implementation	Purpose	Algorithm	Key sizes	Related SFRs
IKE	HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	KAS FFC	DH (dhEphem)	P=2048, SHA2-256	FCS_COP.1/Hash FCS_IPSEC_EXT.1 FCS_RBG_EXT.1

			DSA	L=2048, N=224;
				L=2048, N=256;
				L=3072, N=256	

Certificate signing request generation	HP FutureSmart Firmware OpenSSL 1.1.1	Public/Private key pair generation	RSA	2048; 3072	FIA_X509_EXT.3 FCS_RBG_EXT.1

FCS_CKM.1/SKG (Symmetric key generation)

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

TOE SFRs and compliance rationale

Summary: 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 34 shows the purpose and size of each key generated and the standards to which they conform. For information on how the TOE invokes the DRBG, see the [KMD].

Table 34: Symmetric key generation

Usage	Implementation	Purpose	Key sizes	Standard	Related SFRs
Customer data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	Key generation for customer data encryption	256 bits	NIST SP 800-133 Rev.2 Section 6.1	FCS_RBG_EXT.1 FCS_COP.1/StorageEncryption
Certificate data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	Key generation for certificate data encryption	256 bits	NIST SP 800-133 Rev.2 Section 6.1	FCS_RBG_EXT.1 FCS_COP.1/StorageEncryption

FCS_CKM.2 (Cryptographic Key Establishment)

Objective(s): O.COMMS_PROTECTION, O.STRONG_CRYPTO

Summary: The table below lists various cryptographic key establishment schemes, the corresponding sections of RFC 3526 they comply with, the relevant Security Functional Requirements (SFRs), and the services supported by each scheme.

Table 35: Cryptographic key establishment

Scheme	RFC	SFR	Services
Diffie-Hellman (Group 14)	RFC 3526 Section 3	FCS_IPSEC_EXT.1	Administration, Audit Server, SMB Server, Authentication Server, Time Server, Name Server, Mail Server,
Diffie-Hellman (Group 15)	RFC 3526 Section 4	FCS_IPSEC_EXT.1	

FCS_CKM_EXT.4 (Cryptographic 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):

TOE SFRs and compliance rationale

  - IPsec keys and key material
- Customer data encryption (for O.STORAGE_ENCRYPTION):
  - Passphrase, key-slot key, and master key
- Certificate data encryption (for O.STORAGE_ENCRYPTION):
  - Certificates XML file:
    - Data encryption key
  - Thumbprint files:
    - Master 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.

FCS_CKM.4 (Cryptographic 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):
  - IPsec keys and key material
- Customer data encryption (for O.STORAGE_ENCRYPTION):
  - Passphrase, key-slot key, and master key
- Certificate data encryption (for O.STORAGE_ENCRYPTION):
  - Certificates XML file:
    - Data encryption key
  - Thumbprint files:
    - Master key
    - Data encryption key

Rationale for no nonvolatile key destruction

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

- Customer data encryption:
  - Passphrase — The passphrase is not viewable through any TOE interfaces by either administrators or non-administrators. Additionally, the passphrase is protected by a separate key that is not part of the key chain and that is stored in a protected storage device.
  - Master key — The master key cannot be viewed through any TOE interfaces by administrators or non-administrators. Additionally, the master key is protected by the key-slot key.
- Certificate data encryption:
  - Certificates XML file:

TOE SFRs and compliance rationale

    - Data encryption key — The data encryption key is not viewable through any TOE interfaces by either administrators or non-administrators. The key is never modified, and therefore is never destroyed. Additionally, the data encryption key is protected by a separate key that is not part of the key chain and that is stored in a protected storage device.
  - Thumbprint files:
    - Master key— The master key is not viewable through any TOE interfaces by either administrators or non-administrators. The key is never modified, and therefore is never destroyed. Additionally, the master key is protected by a separate key that is not part of the key chain and that is stored in a protected storage device.
- IPsec:
  - IPsec RSA private key— When an identity certificate and its private key are imported into the TSF's certificate store, or when the TSF generates a private key during the creation of a certificate signing request, the TSF stores the private key in encrypted form on the storage device. For information about the keys used to protect the private key, see the certificate data encryption information above.

Table 36 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 36: 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

TOE SFRs and compliance rationale

IPsec IKE session encrypt key	The IKE session encrypt key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec IKE session authentication key	The IKE session authentication key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec 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 (Customer data encryption)	Used as input into PBKDF2 to derive the key-slot key	RAM	After the key-slot key has been generated	Power off	Power loss
Key-slot key (Customer data encryption)	Used to encrypt/decrypt the master key	RAM	After master key has been encrypted/ unencrypted	Power off	Power loss
Master key (Customer data encryption)	Used to encrypt/decrypt data on customer data partition	RAM	Needed while the HCD is powered on	Power off	Power loss
Data encryption key (Certificates XML file encryption)	Used to encrypt/ decrypt the certificates XML file	RAM	Needed while the HCD is powered on	Power off	Power loss

TOE SFRs and compliance rationale

Master key (Thumbprint files 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
Data encryption key (Thumbprint files 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

FCS_COP.1/DataEncryption (Data Encryption/Decryption)

Objective(s): O.COMMS_PROTECTION, O.STRONG_CRYPTO

Summary: IKE and IPsec support AES CBC 128-bit, AES CBC 192-bit, and AES CBC 256-bit in CBC mode for symmetric data encryption and decryption.

Table 37: AES algorithms

Usage	Implementation	Purpose	Algorithm	Modes	Key sizes	Related SFRs
IKE	HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	Data encryption and decryption	AES	CBC	128 bits, 192 bits, 256 bits	FCS_IPSEC_EXT.1
IPsec	HP FutureSmart Firmware Linux Kernel Crypto API	Data encryption and decryption	AES	CBC	128 bits, 192 bits, 256 bits	FCS_IPSEC_EXT.1

FCS_COP.1/SigGen (Signature Generation and Verification)

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

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 9.1 Cryptographic Module. The RSA signature generation is based on PKCS#1 v1.5 and uses SHA2-256, SHA2-384, and SHA2-512. The RSA signature verification is based on PKCS#1 v1.5 and uses SHA2-256, SHA2-384, and SHA2-512. For more details on IKE, see the TSS for FCS_IPSEC_EXT.1.

TOE SFRs and compliance rationale

The TOE's trusted update function uses the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 for digital signature verification. It utilizes 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.

The TOE’s TSF testing function (dm-verity) uses the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 for digital signature verification. It utilizes 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.

The TOE’s secure boot function uses the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 for digital signature verification. It utilizes the Security Sub-System (SSS) implementation of the RSA 2048-bit algorithm to verify the integrity of the first boot stage, and the HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2) implementation of the same algorithm to verify the integrity of all subsequent boot stages. For more details on secure boot, see the TSS for FPT_SBT_EXT.1.

All implementations meet the [FIPS186-4] standard.

Table 38: Asymmetric algorithms for signature generation/verification

Usage	Implementation	Purpose	Algorithm	Key sizes	Related SFRs
IKE	HP FutureSmart Firmware QuickSec 9.1 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 1.1.1w	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
Secure Boot	HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2)	Signature verification based on PKCS#1 v1.5	RSA	2048 bits	FPT_SBT_EXT.1
	Security Sub-System (SSS)	Signature verification based on PKCS#1 v1.5	RSA	2048 bits	FPT_SBT_EXT.1

FCS_COP.1/Hash (Hash Algorithm)

Objective(s): O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.UPDATE_VERIFICATION, O.STRONG_CRYPTO

Summary:

TOE SFRs and compliance rationale

IKE

IKE supports SHA2-256 for KAS FFC as specified in FCS_CKM.1/AKG.

IKE supports SHA2-256, SHA2-384, and SHA2-512 for RSA signature generation and SHA2-256, SHA2-384, and SHA2-512 for RSA signature verification as specified in FCS_COP.1/SigGen.

Also, IKE supports HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 which use SHA2-256, SHA2-384, and SHA2-512, respectively.

IKE uses the HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module for these algorithms.

IPsec

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

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.

Trusted update

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.

TSF testing

The TOE’s TSF testing function (dm-verity) uses the SHA2-256 algorithm for RSA digital signature verification of the dm-verity root hash and filesystem block integrity checks. This function uses the HP FutureSmart Firmware OpenSSL 1.1.1 implementation of the SHA2-256 algorithm.

Secure boot

The TOE’s secure boot function uses the SHA2-256 algorithm for RSA digital signature verification. This function uses the Security Sub-System (SSS) implementation of SHA2-256 to verify the integrity of the first boot stage, and the HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2) implementation of the SHAs-256 algorithm to verify the integrity of all subsequent boot stages.

Additionally, the secure boot function uses the Security Sub-System (SSS) implementation of SHA2-256 to verify the integrity of whitelisted public keys, as these keys are used to validate the integrity of the first boot stage.

Customer data encryption

The TOE’s customer data encryption feature uses a key-slot key to encrypt (as defined in FCS_COP.1/KeyEnc) the master key stored on the storage device. The key-slot key is derived (as defined in FCS_KDF_EXT.1) from a passphrase using the PBKDF2 algorithm. PBKDF2 uses HMAC-SHA-256 as its pseudorandom function, which is constructed using the SHA2-256 algorithm in the HP FutureSmart Firmware OpenSSL 1.1.1 implementation.

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

Table 39: SHS algorithms

Usage	Implementation	Purpose	Algorithm	Related SFRs
IKE		KAS FFC	SHA2-256	FCS_CKM.1/AKG

TOE SFRs and compliance rationale

	HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	RSA digital signature generation	SHA2-256, SHA2-384, SHA2-512	FCS_COP.1/SigGen
		RSA digital signature verification	SHA2-256, SHA2-384, SHA2-512	
		HMAC	SHA2-256, SHA2-384, SHA2-512	FCS_COP.1/KeyedHash
IPsec	HP FutureSmart Firmware Linux Kernel Crypto API	HMAC	SHA2-256, SHA2-384, SHA2-512	FCS_COP.1/KeyedHash
		HMAC (HMAC_DRBG)	SHA2-256	FCS_COP.1/KeyedHash FCS_RBG_EXT.1
Trusted update	HP FutureSmart Firmware OpenSSL 1.1.1	RSA digital signature verification	SHA2-256	FPT_TUD_EXT.1
Secure Boot	HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2)	RSA digital signature verification	SHA2-256	FPT_SBT_EXT.1
	Security Sub-System (SSS)	RSA digital signature verification	SHA2-256	FPT_SBT_EXT.1
TSF testing	HP FutureSmart Firmware OpenSSL 1.1.1	RSA digital signature verification	SHA2-256	FPT_TST_EXT.1
	HP FutureSmart Firmware Linux Kernel Crypto API	Filesystem block integrity checking using dm-verity		
Customer data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	HMAC (PBKDF2)	SHA2-256	FDP_DSK_EXT.1 FCS_KDF_EXT.1 FCS_COP.1/CMAC

FCS_COP.1/StorageEncryption (Data Encryption/Decryption)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary:

TOE SFRs and compliance rationale

The TOE contains one field-replaceable, nonvolatile storage device, which is an SSD. The TSF ensures that User Document Data and confidential TSF Data are not stored in plaintext on the storage device.

All User Document Data and confidential TSF data are encrypted using AES in CBC mode with a 256-bit key.

For additional details on the encryption of User Document Data and confidential TSF Data stored on the storage device, see the TSS for FDP_DSK_EXT.1.

Table 40: AES encryption/decryption algorithms

Usage	Implementation	Purpose	Algorithm	Key size	Related SFRs
Customer data encryption	HP FutureSmart Firmware Linux Kernel Crypto API	Customer data encryption and decryption	AES-CBC-256	256 bits	FDP_DSK_EXT.1
Certificate data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	Certificate data encryption and decryption	AES-CBC-256	256 bits	FDP_DSK_EXT.1

FCS_COP.1/KeyEnc (Key Encryption)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: The TOE's customer data encryption feature uses a master key to encrypt partitions designated for storing customer data on the storage device. The master key itself is stored on the storage device and is encrypted using the AES-CBC-256 algorithm in the HP FutureSmart Firmware Linux Kernel Crypto API.

For additional details on the keys used for customer data encryption, see the [KMD].

Table 41: Key encryption

Usage	Implementation	Purpose	Algorithm	Key size	Related SFRs
Customer data encryption	HP FutureSmart Firmware Linux Kernel Crypto API	Encryption and decryption of the master key	AES-CBC-256	256 bits	FCS_KYC_EXT.1/CDE

FCS_COP.1/KeyedHash (Keyed Hash Algorithm)

Objective(s): O.COMMS_PROTECTION, O.STRONG_CRYPTO

Summary:

IKE

IKE supports the keyed-hash message authentication algorithms and key sizes specified in Table 42 using the HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module meeting [ISO/IEC 9797-2:2011], Section 7 "MAC Algorithm 2".

TOE SFRs and compliance rationale

IKE uses truncated HMACs. Table 42 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.

IPsec

IPsec support the keyed-hash message authentication algorithms and key sizes specified in Table 42 using the HP FutureSmart Firmware Linux Kernel Crypto API meeting [ISO/IEC 9797-2:2011], Section 7 “MAC Algorithm 2”.

IPsec use truncated HMACs. Table 42 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.

IPsec supports HMAC_DRBG with HMAC-SHA2-256 which uses SHA2-256.

Table 42: HMAC algorithms

Usage	Implementation	Algorithm	Key size	Block size	Output MAC length Actual/Trunc.
IKE	HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	HMAC-SHA2-256-128	256 bits	512 bits	256/128 bits
		HMAC-SHA2-384-192	384 bits	1024 bits	384/192 bits
		HMAC-SHA2-512-256	512 bits	1024 bits	512/256 bits
IPsec	HP FutureSmart Firmware Linux Kernel Crypto API	HMAC-SHA2-256-128	256 bits	512 bits	256/128 bits
		HMAC-SHA2-384-192	384 bits	1024 bits	384/192 bits
		HMAC-SHA2-512-256	512 bits	1024 bits	512/256 bits

FCS_COP.1/CMAC (for cipher-based message authentication)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: The TOE’s customer data encryption feature uses a key-slot key to encrypt (as defined in FCS_COP.1/KeyEnc) the master key stored on the storage device. The key-slot key is derived (as defined in FCS_KDF_EXT.1) from a passphrase using the PBKDF2 algorithm. One of PBKDF2’s primitives is HMAC-SHA-256, which has a key length of 256 bits, a block size of 512 bits, and an output MAC length of 256 bits.

For additional details on the keys used for customer data encryption, see the [KMD].

FCS_IPSEC_EXT.1 (IPsec)

Objective(s): O.COMMS_PROTECTION, O.STRONG_CRYPTO

Summary: In the evaluated configuration, the TOE uses IPsec to protect all communication channels required to satisfy O.COMMS_PROTECTION. The management function for enabling IPsec is specified in the TSS for FMT_MOF.1.

TOE SFRs and compliance rationale
IPsec operates in Transport mode and supports X.509v3 certificates for authentication. It uses the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), and the Internet Key Exchange version 2 (IKEv2). IKEv2 supports the following cryptographic algorithms. • DH (dhEphem) P=2048, SHA2-256 (FCS_CKM.1/AKG) • DSA (FCS_CKM.1/AKG) ○ L=2048, N=224 ○ L=2048, N=256 ○ L=3072, N=256 • RSA 2048-bit and 3072-bit signature generation/verification (FCS_COP.1/SigGen) • AES-CBC-128, AES-CBC-192, and AES-CBC-256 (FCS_COP.1/DataEncryption) • HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1/KeyedHash) • CTR_DRBG(AES) (FCS_RBG_EXT.1) IPsec ESP supports the following cryptographic algorithms. • AES-CBC-128, AES-CBC-192, and AES-CBC-256 (FCS_COP.1/DataEncryption) • HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 (FCS_COP.1/KeyedHash) • HMAC_DRBG (FCS_RBG_EXT.1) In the evaluated configuration, the TOE supports DH Group 14 (2048-bit MODP) and DH Group 15 (3072-bit MODP). These DH groups are specified using defined group parameters as outlined in [RFC3526]. When receiving an IKEv2 proposal, the TOE selects the first DH group from the IKEv2 proposal that matches one of the DH groups configured on the TOE. If no match is found, IKE negotiation fails. When initiating an IKEv2 proposal, the TOE includes all configured DH groups in the proposal, in priority order. The peer then selects the first matching DH group from the proposal that matches its own configuration. If no match is found, the IKE negotiation fails. IKEv2 supports DH/DSA in Phase 1 to establish a protected connection using KAS FFC. The random values required for KAS FFC are generated by the TOE using the CTR_DRBG (AES), as specified in FCS_RBG_EXT.1 and described in the TSS for FCS_RBG_EXT.1. In the IKEv2 exchange, the secret value x is generated using the CTR_DRBG (AES) in the HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module. The length of x is at least twice the security strength of the negotiated Diffie-Hellman group (112 bits for DH Group 14 (2048-bit MODP) and 128 bits for DH Group 15 (3072-bit MODP)). Nonces (256-bits in length) are generated using the same CTR_DRBG (AES), with a length at least equal to the security strength of the negotiated Diffie-Hellman group (112 bits for DH Group 14 (2048-bit MODP) and 128 bits for DH Group 15 (3072-bit MODP)) and at least half the output size of the negotiated PRF hash. IKEv2 Security Association (SA) lifetimes can be established based on time. Phase 1 SA lifetimes can be limited to a maximum of 24 hours, while Phase 2 (Child SA) lifetimes can be limited to a maximum of 8 hours. The TOE supports peer authentication using RSA-based digital signatures with 2048-bit and 3072-bit keys. Encrypted IKEv2 payloads are required to use either AES-CBC-128, AES-CBC-192, or AES-CBC-256, providing

TOE SFRs and compliance rationale

128-bit, 192-bit, and 256-bit security strength, respectively. No other encryption algorithms are allowed in the evaluated configuration.

The TOE supports the following reference identifier types for IPsec peers: Distinguished Name, SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), and SAN: Email. However, only one identifier type and value can be configured per IPsec peer on the TOE. When the TOE receives a peer's certificate, it checks whether the configured identifier type is present. If found, the TOE uses the corresponding value as the peer's presented identifier for authentication. If the configured identifier type is not found in the certificate, peer authentication fails.

The TOE supports AES-CBC-128, AES-CBC-192, and AES-CBC-256 for encrypting IPsec ESP payloads, providing 128-bit, 192-bit, and 256-bit security strength, respectively. No other encryption algorithms are permitted in the evaluated configuration. The administrator must configure the TOE to use an IKE encryption algorithm whose security strength is equal to or greater than that of the algorithm used for IPsec ESP.

IKEv2 and IPsec are conformant to the MUST/MUST NOT requirements of the following Internet Engineering Task Force (IETF) Request for Comments (RFCs).

- [RFC3602] for use of AES-CBC-128, AES-CBC-192, and AES-CBC-256 in IPsec
- [RFC4301] for IPsec
- [RFC4303] for ESP
- [RFC4304] for extended sequence numbers
- [RFC2407] and [RFC2408] for ISAKMP
- [RFC4306], [RFC4718], [RFC5996], and [RFC3526] for IKEv2
- [RFC4868] for SHA-2 HMAC in IPsec

All cryptographic functions used by IKE are implemented in the HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module. All cryptographic functions used by IPsec ESP are implemented in the HP FutureSmart Firmware Linux Kernel Crypto API.

Packet processing

In a network context, the TOE is an endpoint versus being an intermediary such as a network switch. Thus, packets originate from and terminate at the TOE.

When the TOE receives an incoming packet, it first determines whether the packet is destined for the TOE. If it is not, the packet is discarded. If it is, the TOE applies the IPsec rules defined in the SPD, which map address templates to service templates—effectively mapping IP addresses to ports or services. If a matching IPsec rule requires protection and no corresponding Security Association (SA) exists, the TOE discards the packet and, if the packet is a request to initiate a connection, initiates an IKE negotiation to establish the necessary SA. Once the SA is established, subsequent packets that match the policy are decrypted, authenticated, and processed as part of the associated secure connection.

For outgoing packets originating from the TOE, the TOE similarly applies the SPD to determine whether protection is required. If a matching IPsec rule requires protection and an appropriate SA exists, the packet is encrypted and authenticated using the parameters of the SA before transmission. If no SA exists, the TOE initiates IKE negotiation to establish the SA before subsequent packets in the flow are transmitted.

TOE SFRs and compliance rationale

When a packet matches an IPsec rule and an appropriate Security Association (SA) exists—whether in the outgoing or incoming case—the TOE verifies that the SA's lifetime has not expired and that its data transmission limits have not been exceeded. If any of these checks fail, the packet is discarded. If all checks pass, the packet is considered valid for IPsec processing and is forwarded as part of the associated secure connection.

In both incoming and outgoing cases, any packet that does not match a defined IPsec rule is processed according to the final built-in rule in the SPD. In the evaluated configuration, this default rule is configured to discard unmatched packets. Additionally, packets that are not IPsec-protected are also discarded, except for DHCPv4/BOOTP, and ICMPv4 packets, which are explicitly permitted (i.e., allowed to bypass IPsec processing) in the evaluated configuration.

The TOE's straightforward IPsec rule configuration minimizes the possibility of overlapping rules. However, if overlapping rules exist, the first matching rule in the list is enforced. Administrators can add, delete, enable, or disable rules, as well as change the processing order of existing rules.

FCS_KDF_EXT.1 (Cryptographic Key Derivation)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: As described in the TSS for FCS_KYC_EXT.1/CDE, the TOE's customer data encryption feature employs a key chain consisting of a passphrase, a key-slot key, and a master key. The TSF derives the key-slot key using PBKDF2 (as specified in FCS_KDF_EXT.1), with the passphrase as input. The passphrase is a submask generated by an RBG, as a specified in FCS_CKM.1/SKG.

The PBKDF2 algorithm conforms to [NIST SP 800-132].

For additional details on the keys used by the customer data encryption feature, see the [KMD].

FCS_KYC_EXT.1/CDE (Key chaining)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: The TSF implements a feature called customer data encryption, which encrypts the partitions on the storage device designated for customer data. In the evaluated configuration, this feature uses the AES-CBC-256 algorithm for encryption. For more details on the customer data encryption feature, see the TSS for FDP_DSK_EXT.1.

The key chain for this feature consists of:

- Passphrase (256 bits)
- Key-slot key (256 bits)
- Master key (256 bits)

The master key is used to encrypt (as specified in FCS_COP.1/StorageEncryption) the customer data partitions on the storage device. It is stored on the same drive, encrypted (as specified in FCS_COP.1/KeyEnc) with the AES-CBC-256 algorithm using the key-slot key.

The passphrase is stored in nonvolatile memory and protected by another key that is not part of the key chain.

The master key and the passphrase are regenerated (as specified in FCS_CKM.1/SKG) by the CTR_DRBG (AES) algorithm on every HCD boot.

TOE SFRs and compliance rationale

The key-slot key is derived (as specified in FCS_KDF_EXT.1) using the PBKDF2 algorithm from the passphrase. It is regenerated during every HCD boot.

In the evaluated configuration, the key chain supports a master key output of no fewer than 256 bits.

For more details about the key chain and how the passphrase is protected by another key that is not part of the key chain, see [KMD].

FCS_KYC_EXT.1/CM (Key chaining)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: The TSF stores the IPsec identity certificate and its corresponding private key in encrypted form in a certificates XML file stored on the storage device. This file is encrypted using the AES-CBC-256 algorithm.

The key chain for this feature consists of:

- Data encryption key (256 bits)

The data encryption key is used to encrypt (as specified in FCS_COP.1/StorageEncryption) the certificates XML file stored on the storage device using the AES-CBC-256 algorithm. This key is stored in nonvolatile memory and protected by another key that is not part of the key chain.

The data encryption key is generated (as specified in FCS_CKM.1/SKG) using the CTR_DRBG (AES) algorithm when the HCD is powered on for the first time.

The key chain supports a data encryption key output of no fewer than 256 bits.

For more details about the key chain and how the data encryption key is protected by another key that is not part of the key chain, see [KMD].

FCS_KYC_EXT.1/CMT (Key chaining)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

Summary: The TSF stores identity certificates and their corresponding private keys in individual files (a.k.a., thumbprint files), which are stored in encrypted form on the storage device. These thumbprint files are encrypted using the AES-CBC-256 algorithm.

The key chain for this feature consists of:

- Data encryption key (256 bits)
- Master key (256 bits)

The data encryption key is used to encrypt (as specified in FCS_COP.1/StorageEncryption) the individual thumbprint files stored on the storage device using the AES-CBC-256 algorithm. This key is regenerated (as specified in FCS_SMC_EXT.1) during every HCD boot by combining the master key and a submask through an XOR operation.

The master key is stored in nonvolatile memory and protected by another key that is not part of the key chain. This key is generated (as specified in FCS_CKM.1/SKG) using the CTR_DRBG (AES) algorithm when the HCD is powered on for the first time.

The submask is generated outside the HCD and embedded in the TOE firmware.

TOE SFRs and compliance rationale

The key chain supports a data encryption key output of no fewer than 256 bits.

For more details about the key chain and how the master key is protected by another key that is not part of the key chain, see [KMD].

FCS_RBG_EXT.1 (Random Bit Generation)

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

Summary: The following table outlines the DRBGs used by the TSF and their respective usages.

Table 43: DRBG algorithms

Usage	Implementation	Algorithm	Hardware noise sources	Minimum entropy bits	Related SFRs
IKE	HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	CTR_DRBG (AES)	1	256 bits	FCS_CKM.1/AKG FCS_COP.1/DataEncryption FCS_IPSEC_EXT.1
IPsec	HP FutureSmart Firmware Linux Kernel Crypto API	HMAC_DRBG (HMAC-SHA2-256)	1	256 bits	FCS_CKM.1/AKG FCS_COP.1/KeyedHash FCS_COP.1/DataEncryption FCS_IPSEC_EXT.1
Customer data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	CTR_DRBG (AES)	1	256 bits	FCS_CKM.1/SKG FCS_COP.1/StorageEncryption FDP_DSK_EXT.1
Certificate data encryption	HP FutureSmart Firmware OpenSSL 1.1.1	CTR_DRBG (AES)	1	256 bits	FCS_CKM.1/SKG FCS_COP.1/StorageEncryption FDP_DSK_EXT.1
Certificate signing request	HP FutureSmart Firmware OpenSSL 1.1.1	CTR_DRBG (AES)	1	256 bits	FCS_CKM.1/AKG FIA_X509_EXT.3.1

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

FCS_SMC_EXT.1(Submask Combining)

Objective(s): O.STORAGE_ENCRYPTION, O.STRONG_CRYPTO

TOE SFRs and compliance rationale

Summary: The TSF stores identity certificates and their corresponding private keys in encrypted individual files (a.k.a., thumbprint files) on the storage device.

The TSF combines a 256-bit master key and a 256-bit submask using an XOR operation to generate the 256-bit data encryption key used to encrypt the thumbprint files.

FDP_ACC.1 (Subset access control)

Objective(s): O.ACCESS_CONTROL, O.USER_AUTHORIZATION

Summary: [HCDcPP] predefines the subjects, objects, and operations. Table 19 and Table 20 of this ST list these values and enumerates the operations between the subjects and objects.

FDP_ACF.1 (Security attribute based access control)

Objective(s): O.ACCESS_CONTROL, O.USER_AUTHORIZATION

Summary: In this section, Table 19 is explained first followed by Table 20.

Print Create D.USER.DOC in Table 19

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 19 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.

Required security attributes:

- Subject: None (Unauthenticated user)
- Object: Job owner

Print Read/Modify/Delete D.USER.DOC in Table 19

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 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.

Required security attributes:

- Subject: Control Panel user identity/role
- Object: Job owner

Storage / retrieval Create/Read/Modify/Delete D.USER.DOC in Table 19

Print jobs can be stored in Job Storage.

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

TOE SFRs and compliance rationale

print job in Job Storage. This is why "allowed" is shown for "create" in Table 19 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.

Required security attributes:

- Subject: Unauthenticated users (create print job only) or Control Panel user identity/role
- Object: Job owner

Print Create/Read/Modify/Delete D.USER.JOB in Table 20

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.

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.

Only the job owner and U.ADMIN can delete the print job of a job owned by the job owner.

By design, the D.USER.JOB information of a print job cannot be modified by anyone.

Required security attributes:

- Subject: Unauthenticated user (create print job and view print queue only) or Control Panel user identity/role
- Object: Job owner

Storage / retrieval Create/Read/Modify/Delete D.USER.JOB in Table 20

Print jobs can be stored in Job Storage.

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 20 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 D.USER.JOB information of a print job stored in Job Storage cannot be modified.

Required security attributes:

- Subject: Unauthenticated users (create print job only) or Control Panel user identity/role
- Object: Job owner

FDP_DSK_EXT.1 (Protection of Data on Disk)

Objective(s): O.STORAGE_ENCRYPTION

Summary: The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an SSD. The TOE performs encryption of User Document Data and confidential TSF data according to FCS_COP.1/StorageEncryption without any user intervention.

TOE SFRs and compliance rationale
The encryption and decryption functions are integrated into the TOE firmware and are automatically activated on the first boot after the printer is received from the factory. The TSF encrypts the customer data partitions. For additional details, refer to the Customer Data Encryption section below. The private key associated with the IPsec identity certificate, used for IPsec functionality, is stored outside the customer data partitions and is also encrypted. For further information, see the Certificate Data Encryption section below. All other sections and partitions of the storage device are not encrypted. *Customer Data Encryption* The TSF implements a feature called customer data encryption, which is based on the device-mapper crypt (dm-crypt) target and uses Linux Unified Key Setup (LUKS) format for key management and encryption metadata. dm-crypt provides transparent encryption of block devices using the HP FutureSmart Firmware Linux Kernel Crypto API. The customer data encryption feature protects customer data (including User Document Data) by encrypting the partitions on the storage device designated for customer data. In the evaluated configuration, these partitions are encrypted using the AES-CBC-256 implementation in the HP FutureSmart Firmware Linux Kernel Crypto API. Data stored on the encrypted partition includes stored jobs (e.g., print), temporary job files, PJL and PostScript filesystem files including downloaded fonts, and extensibility customer data (if stored there by the extensibility solution). On every HCD boot, the customer partitions (LUKS-encrypted volumes) are recreated and reformatted. This process effectively performs a cryptographic erase of all data previously stored on these partitions. *Certificate Data Encryption* The TSF encrypts identity certificates and their corresponding private keys on the storage device. Certificates XML file: The IPsec identity certificate and its corresponding private key are stored in encrypted form in a certificates XML file stored on the storage device. They are encrypted using the AES-CBC-256 implementation in HP FutureSmart Firmware OpenSSL 1.1.1. The data encryption key is generated using the CTR_DRBG implementation in HP FutureSmart Firmware OpenSSL 1.1.1 when the HCD is powered on for the first time. Thumbprint files: When an identity certificate and its private key are imported, the TSF stores them together in a file (a.k.a., thumbprint file) that is encrypted on the storage device. Each thumbprint file is individually encrypted using AES-CBC-256 implementation in HP FutureSmart Firmware OpenSSL 1.1.1. The data encryption key is generated during every HCD boot by combining a master key and a submask through an XOR operation. The master key is generated using the CTR_DRBG implementation in HP FutureSmart Firmware OpenSSL 1.1.1 when the HCD is powered on for the first time. For additional details on the keys used to encrypt certificate data, see the [KMD].
FIA_AFL.1 (Authentication failure handling)
Objective(s): O.USER_I&A, O.AUTH_FAILURES

TOE SFRs and compliance rationale

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.

The lockout mechanism uses the following control values.

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

The account lockout maximum attempts value allows an administrator to control the number of failed authentication attempts on 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.

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

The account reset lockout counter interval value allows an administrator to specify the time (in seconds) in which the failed login attempts must occur before the account lockout maximum attempts counter is reset to zero. This value must be equal to or greater than the account lockout interval value.

FIA_ATD.1 (User attribute definition)

Objective(s): O.USER_AUTHORIZATION

Summary:

Control Panel users

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

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

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.

EWS users

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

TOE SFRs and compliance rationale

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

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

REST users

The REST interface is an administrator-only interface used to manage the TOE over IPsec.

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.

FIA_PMG_EXT.1 (Password management)

Objective(s): O.USER_I&A

Summary: The TOE manages the Device Administrator Password.

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.

The Device Administrator Password is used by the Control Panel, EWS, and REST interfaces, and can be managed through the EWS.

FIA_UAU.1 (Timing of authentication)

Objective(s): O.USER.I&A

Summary:

Control Panel

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

- 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

TOE SFRs and compliance rationale

- 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

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

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

- Internal Authentication method
    - Local Device Sign In
- External Authentication methods
    - LDAP Sign In
    - Windows Sign In (via Kerberos)

The Local Device Sign In method is always available in the TOE. Local Device Sign In contains only one account—the built-in Device Administrator account—in the evaluated configuration. The username (display name) and password are maintained internally by the TOE. At the Control Panel, the user selects the Local Device Sign In method, selects Administrator Access Code (a.k.a. Device Administrator account) from a menu, and is then prompted for the Device Administrator Password.

If an LDAP Sign In method is configured, that method will be one of the possible External Authentication methods displayed in the menu. This method allows for the use of an LDAP server, such as the Microsoft Active Directory server, for I&A. Both the username and password are maintained by the LDAP server. The TOE uses the LDAP version 3 protocol over IPsec to communicate to the LDAP server. If a user selects this method, the user must enter a valid LDAP account's username and password to be granted access to the TOE.

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

Network interfaces

Most of the client network interfaces protected by IPsec perform authentication. The following table 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 44: IPsec client interfaces

IPsec client interface	Authentication?	TSF-mediated actions prior to authentication?
PJL (a.k.a. P9100)	No	n/a

TOE SFRs and compliance rationale

EWS	Yes	Select a sign in method
REST	Yes	• 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

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 print job. The TOE does not require authentication of this username. Table 44 shows any TSF-mediated actions prior to authentication for this protocol.

EWS over IPsec

The EWS interface is a web browser-based administrative interface used to manage the TOE over IPsec. The EWS interface requires the user to sign in using the same sign in method menu options as provided by the Control Panel (i.e., Local Device Sign In, LDAP Sign In, and Windows Sign In when configured for these sign in methods). Table 44 shows any TSF-mediated actions prior to authentication for this protocol.

REST over IPsec

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

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 44 shows any TSF-mediated actions prior to authentication for this protocol.

Other

Also see the TSS for FIA_UID.1.

FIA_UAU.7 (Protected authentication feedback)

Objective(s): O.USER.I&A

TOE SFRs and compliance rationale

Summary: 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.

FIA_UID.1 (Timing of identification)

Objective(s): O.ADMIN_ROLES, O.USER.I&A

Summary: From the Control Panel, the user can perform the following actions prior to identification.

- 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

Once the IPsec channel is successfully established, the following interfaces initiate their identification mechanisms. The following shows their TSF-mediated actions prior to identification.

- 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

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

For additional information on I&A, see the TSS for FIA_UAU.1.

FIA_USB.1 (User-subject binding)

Objective(s): O.USER.I&A

TOE SFRs and compliance rationale

Summary:

Control Panel User Identity Binding

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

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

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

Control Panel and EWS User Role Binding

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

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

Device Administrator session PS = Device Administrator PS.

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

External user accounts introduce the concept of network groups. A network group (a.k.a. group) is a collection of zero or more external user accounts. Each External Authentication method defines and maintains its own groups. The members of a group are comprised of the external user accounts from that External Authentication method. An external user account can be associated with zero or more groups.

A TOE administrator can associate zero or one PS to each group and zero or one PS to each external user account. These PS associations are stored and maintained on the TOE. A TOE administrator can create, modify, and delete these associations. By default, there are no PS associations for external user accounts and groups. For more information on the TOE's permission set association management, see the TSS for FMT_MSA.1.

A PS is associated with each External Authentication method. These associations are also stored and maintained on the TOE. A TOE administrator can modify these associations.

The TOE combines these various PSs using one of the following three methods.

Method #1: If the external user account has a PS association, then the TOE combines the external user account's PS and the Device Guest PS to create the external user's session PS.

User session PS = External user account PS + Device Guest PS.

TOE SFRs and compliance rationale

Method #2: If the external user account does not have an associated PS, the TOE obtains the groups to which the external user account is a member. For each of these groups, the TOE looks for matching group-to-PS associations. For each group-to-PS association match, the TOE combines that group's PS with any previously found group PSs. Once all matches have been found, the TOE combines these group PSs with the Device Guest PS to create the external user's session PS.

User session PS = Network group PSs + Device Guest PS.

Method #3: If there are no group-to-PS associations found for the external user account and the external user account does not have an associated PS, then the TOE combines the External Authentication method's PS and the Device Guest PS to create the external user's session PS.

User session PS = External Authentication method PS + Device Guest PS.

An administrator can associate one sign in method to a Control Panel application. This association limits the application to run only when the user signs in using the associated sign in method. For example, if an application is only associated with the LDAP Sign In method, a user must sign in using the LDAP Sign In method in order to run that application. The enforcement of this association is controlled by the "Allow users to choose alternate sign-in methods 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.

Remote User Identity Binding

Once an IPsec client computer has performed a successful IPsec connection with the TOE, the TOE uses the client's IP address as the client's user identifier for IPsec-related audit records.

The EWS and REST interfaces support I&A mechanisms and use some form of username (e.g., Display name, Windows username) in audit records.

In the case of EWS, the interface provides the same options as the Control Panel for sign in methods. Because of this, the EWS identity will be the Display name if the Local Device Sign In method is selected by the user, the LDAP username if the LDAP Sign In method is selected by the user, or the Windows username if the Windows Sign In method is selected by the user. From an auditing and access control perspective, the IP address is used by IPsec when generating IPsec-related and network-related audit records. The EWS identity (i.e., Display name, LDAP username, Windows username) is used for all other identity-related purposes such as management-related tasks and audit records and access control enforcement and audit records.

In the case of the 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.

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.

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

TOE SFRs and compliance rationale
user identity of the client computer. The IP address of the client computer is the user identity of the client computer. *Remote User Role Binding* In the case of EWS, the role is determined by the login account used by the user when logging in to the EWS interface. In the case of PJL, the PJL interface only supports unauthenticated users. No specific role exists for these users. 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. *Other* 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.
FIA_X509_EXT.1 (X.509 Certificate Validation)
Objective(s): O.COMMS_PROTECTION **Summary**: The TOE performs X.509 certificate validation to support IPsec ESP during peer authentication. It determines the validity of the IPsec peer's certificate by ensuring that both the certificate and its path are valid in accordance with RFC 5280 with a minimum path length of three certificates. Additionally, it ensures that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE, and that the path terminates with a trusted CA certificate. The TOE supports OCSP to verify the revocation status of an IPsec's peer X.509 certificate during IPsec peer authentication. This applies only when the peer's certificate includes the AIA extension specifying an OCSP responder. If the OCSP revocation check fails, or if the peer's certificate is revoked, the TOE will reject the certificate and terminate the connection attempt. When performing OCSP checks, the TOE verifies that the certificate used to sign the OCSP response includes the OCSP Signing purpose in the extendedKeyUsage field.
FIA_X509_EXT.2 (X.509 Certificate Authentication)
Objective(s): O.COMMS_PROTECTION **Summary**: The TOE supports multiple X.509 identity certificates in its certificate store; however, only one is designated for IPsec and used during IPsec peer authentication. The [CCECG] section Certificates provides instructions on how to designate an X.509 identity certificate for IPsec usage. If TOE's validation of an IPsec peer's X.509 certificate during IPsec peer authentication fails, the TOE will reject the certificate and terminate the connection attempt. By default, OCSP certificate revocation checks for IPsec peer authentication are disabled. In the evaluated configuration, these checks must be enabled. The [CCECG] section Certificates provides instructions on how to enable them.
FIA_X509_EXT.3 (X.509 Certificate Requests)
Objective(s): O.COMMS_PROTECTION

TOE SFRs and compliance rationale

Summary: An X.509 Certificate Request can be generated through the TOE’s EWS interface. The X.509 Certificate Request, generated by the TSF, conforms to RFC 2986 and includes the public key. It may also contain fields such as Common Name, Organization, Organizational Unit, Country, State, and Locality. Before installing the CA-generated and signed X.509 certificate in its certificate store, the TSF validates the certificate chain in the X.509 Certificate Response.

FMT_MOF.1 (Management of security functions behavior)

Objective(s): O.ADMIN_ROLES

Summary:

Allow users to choose alternate sign-in methods at the product control panel: With the “Allow users to choose alternate sign-in methods at the product control panel” function, the TOE provides an administrator the ability to enable and disable this function. When this function is disabled, it requires the user to sign in using the sign-in method associated with the selected application in order to access that application. This function is restricted to U.ADMIN and can be performed through the EWS interface. For related information, see the TSS for FIA_USB.1.

Control Panel 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.

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

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

Account lockout: With the account lockout function, the TOE provides an administrator the ability to enable and disable the account lockout 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.

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.

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.

TOE SFRs and compliance rationale

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.

FMT_MSA.1 (Management of security attributes)

Objective(s): O.ACCESS_CONTROL, O.USER_AUTHORIZATION

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.

- Control Panel and EWS subject attributes (identities and roles)
- Job Storage object attributes

Control Panel and EWS identities

The TOE's access control mechanism uses the identities supplied by the Control Panel and EWS interfaces to control access to objects. This makes identities a subject security attribute of the access control mechanism.

The TOE supports both Internal and External Authentication mechanisms in the evaluated configuration.

Account identity (Internal Authentication mechanism): The 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, 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 22. Because there are no management operations, the authorized roles entry is marked as not applicable (n/a) in Table 22. There is no default value property for the Display name because the account is predefined, thus, Table 22 shows this as not applicable (n/a). Similarly, no role can override the default value.

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 22. Because the TOE has no control over these external account identities, there is no default value property (marked as n/a in Table 22) and no default value to override, thus, no role can override the default value.

Control Panel and EWS roles

The TOE's access control mechanism also uses permission sets to control access to objects on the TOE. Permission sets are used to determine user roles on the TOE. The TSS for FMT_SMR.1 contains an explanation of permission sets. Permission sets can be associated with internal user accounts, external user accounts (network users), network groups, and to External Authentication mechanisms. When a user logs in via the Control Panel or EWS, the user's session permission set is calculated by the TOE based on the rules described in the TSS for

TOE SFRs and compliance rationale
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. ***Device Administrator permission set permissions***: For the Device Administrator permission set permissions, the TOE provides the "view" management operation. This management operation is restricted to U.ADMIN. This permission set comes predefined in the TOE. Its default value property is considered permissive because its predefined value allows access to everything. Because this value is predefined, there is no default value override role associated with it. ***Device User and Device Guest permission set permissions***: For the Device User permission set permissions and the Device Guest permission set permissions, the TOE provides the "modify and view" management operations. These management operations are restricted to U.ADMIN. These permission sets come predefined in the TOE. Their default value properties are considered restrictive because their predefined values are more restrictive than the Device Administrator permission set. Because these values are predefined, there is no default value override role associated with them. ***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. *Job Storage ownerships* Ownership (job 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. ***Job owner***: For job 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 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.
FMT_MSA.3 (Static attribute initialization)
Objective(s): O.ACCESS_CONTROL, O.USER_AUTHORIZATION **Summary**: The descriptions have been provided in the TSS for FMT_MSA.1.
FMT_MTD.1 (Management of TSF data)
Objective(s): O.ACCESS_CONTROL **Summary**: *TSF Data owned by U.NORMAL or associated with Documents or jobs owned by a U.NORMAL* **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. *List of TSF Data not owned by U.NORMAL*

TOE SFRs and compliance rationale

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.

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

Permission set associations (only on the Device Administrator account): The Device Administrator account is the only internal, built-in account in the evaluated configuration. This account has the Device Administrator permission set permanently associated with it. The only management operation provided for the Device Administrator account's permission set association is the "view" operation. This can only be performed by a U.ADMIN (including the Device Administrator). For related information, see the TSS for FDP_ACF.1 and TSS for FMT_MSA.1.

Note: Although audit records are TSF Data not owned by U.NORMAL, the TOE does not provide the ability to management audit records.

List of software, firmware, and related configuration data

IPsec CA and identity certificates: For the IPsec CA certificates, the TOE provides the "import and delete" operations through the EWS interface. The import operation adds a CA certificate to the TOE. The delete operation removes the selected CA certificate from the TOE. These operations are restricted to U.ADMIN. The TOE may contain one or more CA certificates.

For the IPsec identity certificates, the TOE provides the "import and delete" operations for CA-signed identity certificates through the EWS interface. The import operation adds a CA-signed identity certificate to the TOE. The delete operation removes the CA-signed identity certificate from the TOE. These operations are restricted to U.ADMIN.

The TOE initially comes with a self-signed identity certificate for IPsec. This self-signed identity certificate is generated during manufacturing of the TOE and cannot be deleted. This self-signed identity certificate must not be used in the evaluated configuration. Instead, the [CCECG] section Certificates instructs the U.ADMIN to import a CA-signed identity certificate and to set this CA-signed identity certificate as the TOE's IPsec certificate. The TOE only allows one certificate to be its IPsec certificate.

IPsec policy: The TOE allows administrators to manage the IPsec policy, which includes rules, address templates, service templates, IPsec templates, and advanced settings to secure incoming and outgoing data exchanges. Each rule consists of an address template, a service template, and an action-on-match, which can be set to allow, drop, or require IPsec protection. If require IPsec protection is selected, the rule must be associated with an IPsec template. In the evaluated configuration, all rules, except the default rule, must be set to require IPsec protection. The default rule must be set to drop (i.e., discard packets).

Management of the IPsec policy includes the “change”, “view”, “add”, and “delete” operations. These operations are performed through the TOE’s EWS interface and are restricted to U.ADMIN.

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

TOE SFRs and compliance rationale
operation is restricted to U.ADMIN. For related information, see the TSS for FPT_STM.1. The NTS server function must be enabled for the NTS server configuration data to have an effect. For more information on the NTS server enablement, see the "Automatically synchronize with a Network Time Service" function in the TSS for FMT_MOF.1. ***Minimum password length***: For the minimum password length setting, the TOE provides the "change" operation. The TOE provides the 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. ***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. ***Account lockout interval***: For the account lockout interval value, the TOE provides the "change" operation. This value allows an administrator to control the length of time that the account remains locked. The administrator can choose a value between 60 and 1800 seconds inclusively in the evaluated configuration. The account lockout interval value affects the Device Administrator account. The change operation is restricted to U.ADMIN. For more information on account lockout in general, see the TSS for FIA_AFL.1. The account lockout function must be enabled for the account lockout interval value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1. ***Account reset lockout counter interval***: For the account reset lockout counter interval value, the TOE provides the "change" operation. This value allows an administrator to specify the time (in seconds) in which the failed login attempts must occur before the account lockout maximum attempts counter is reset. This value must be equal to or greater than the account lockout interval value. The account reset lockout counter interval value affects the Device Administrator account. The change operation is restricted to U.ADMIN. For more information on account lockout in general, see the TSS for FIA_AFL.1. The account lockout function must be enabled for the account reset lockout counter interval value to have an effect. For information on the account lockout enablement function, see the TSS for FMT_MOF.1. ***Session inactivity timeout***: For the session inactivity timeout, the TOE provides the "change" operation. The change operation allows an administrator to change the amount of time of inactivity before automatically logging out the user from an interactive session. This timeout works for both Control Panel and EWS sessions. The Control Panel and EWS interfaces have independent session inactivity timeout values. The change operation is restricted to U.ADMIN for both interfaces. For related information, see the TSS for FTA_SSL.3.
FMT_SMF.1 (Specification of Management Functions)
Objective(s): O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION

TOE SFRs and compliance rationale

Summary: Table 24 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.

FMT_SMR.1 (Security roles)

Objective(s): O.ACCESS_CONTROL, O.ADMIN_ROLES, O.USER_AUTHORIZATION

Summary: The TOE supports two roles:

- U.ADMIN
- U.NORMAL

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.

Permission sets

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 pages 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 page.

The TOE contains the following built-in permission sets.

- Device Administrator—Grants administrative capabilities
- Device User—Grants typical user capabilities
- Device Guest—Grants capabilities to non-signed in users

These built-in permission sets cannot be renamed or deleted. The Device Administrator permission set cannot be modified, but an administrator can modify the permissions in the Device User and Device Guest permission sets. In the evaluated configuration, the Device Guest permission set is empty (i.e., contains no permissions) by default. (Device Guest is mentioned here because its definition is used in the TSS for FIA_USB.1.)

As an alternative to built-in permission sets, administrators can create custom permission sets that allow an administrator to better map the TOE's permissions to the usage model of their organization. Administrators can also modify and delete any existing custom permission sets. By default, the TOE comes with no custom permission sets.

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

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

All permission sets are stored and maintained locally on the TOE. This means that the permission sets for the internal user accounts, external user accounts, authentication mechanisms, and network groups are all stored and maintained locally on the TOE.

TOE SFRs and compliance rationale

FPT_SBT_EXT.1 (Secure Boot)

Objective(s): O.FW_INTEGRITY

Summary: The TSF implements secure boot with an immutable hardware root of trust provided by ROM.

SHA2-256 hashes of public keys are stored in ROM, and each key has a corresponding OTP bit that designates it as enabled or disabled.

When power is applied to the HCD, the boot code in ROM executes first. It checks the OTP bits to identify enabled public keys and generates a whitelist of valid ones. Using the SHA2-256 hash of a valid key stored in ROM, the boot ROM verifies the public key associated with the digital signature of the first boot stage. If the public key is successfully authenticated, the boot ROM then verifies the integrity of the first boot stage using that public key and its digital signature.

The first boot stage then verifies the integrity of the next boot stage, and each subsequent stage continues this process, verifying the integrity of the stage that follows. Each boot stage is verified using digital signature verification.

If a boot stage verification fails, the TSF halts the boot process to prevent the execution of untrusted code and reboots the HCD. Upon reboot, the TSF halts the boot process, and displays an error message on the Control Panel UI. The administrator can then use the Control Panel UI to reinstall the TOE image.

The integrity of each boot stage is verified by checking its digital signature using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5. The Security Sub-System (SSS) implements both the RSA 2048-bit and SHA2-256 algorithms to verify the integrity of the first boot stage, while the HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2) implementation of the same algorithms is used to verify the integrity of all subsequent boot stages. For additional details on these algorithms, see the TSS for FCS_COP.1/SigGen and TSS for FCS_COP.1/Hash.

FPT_KYP_EXT.1 (Protection of Key and Key Material)

Objective(s): O.KEY_MATERIAL, O.STRONG_CRYPTO

Summary:

As per the TSS for FCS_KYC_EXT.1/CDE, the key chain for the customer data encryption feature consists of the master key, passphrase, and key-slot key. Only the master key and passphrase are stored in nonvolatile storage memory. The master key is encrypted (as specified in FCS_COP.1/KeyEnc) using the key-slot key, while the passphrase is protected by a separate key that is not part of the key chain and is stored on a protected storage device.

As per the TSS for FCS_KYC_EXT.1/CM, the key chain for encrypting the certificates XML file consists of a single key, the data encryption key. This key is stored in nonvolatile memory and is protected by another key, which is not part of the key chain and is stored on a protected storage device.

As per the TSS for FCS_KYC_EXT.1/CMT, the key chain for encrypting thumbprint files consists of a master key and a data encryption key. Only the master key is stored in nonvolatile memory. The master key is stored in nonvolatile memory and is protected by another key that is not part of the key chain and is stored on a protected storage device.

FPT_SKP_EXT.1 (Protection of TSF Data)

TOE SFRs and compliance rationale
Objective(s): O.COMMS_PROTECTION **Summary**: The TOE is a closed system and does not provide an interface to symmetric or asymmetric keys. As a closed system, it prevents administrators from reading memory or directly accessing storage. Ephemeral asymmetric and symmetric keys generated and used in IPsec sessions are inaccessible to any user, as the TOE does not provide a user interface to read memory. The TOE's private asymmetric keys associated with X.509v3 certificates used by IPsec are inaccessible to any user, as they are neither displayed nor exportable in the evaluated configuration.
FPT_STM.1 (Reliable time stamps)
Objective(s): O.AUDIT, O.STRONG_CRYPTO **Summary**: Although [HCDcPP] only maps O.AUDIT and O.STRONG_CRYPTO to FPT_STM.1, it is worth noting that reliable timestamps are also used by O.COMMS_PROTECTION and O.UPDATE_VERIFICATION when validating the validity period of certificates and by O.USER_I&A when performing session inactivity timeouts and authentication failure handling. The TOE contains an internal system clock that is used to generate reliable timestamps. The TOE requires the use of an NTS service to keep the internal system clock's time synchronized. Only administrators can manage the system clock and the TOE's configuration of NTS.
FPT_TST_EXT.1 (TSF testing)
Objective(s): O.TSF_SELF_TEST **Summary**: The TOE supports dm-verity to verify the integrity of SquashFS filesystem firmware images, helping ensure the correct operation of the TSF during startup. At each boot, the TSF verifies the digital signature of the dm-verity root hash corresponding to a SquashFS firmware image. During operation (including boot time), dm-verity verifies the integrity of each filesystem block before loading it into memory by comparing it to the authenticated hash tree. If the digital signature verification of the dm-verity root hash fails, or if a file system block integrity check fails during boot, the TSF halts the boot process. The administrator can then use the Control Panel UI to reinstall the TOE firmware. The digital signature of the dm-verity root hash is verified using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5, while the hashes of the filesystem blocks are verified using SHA2-256. The TSF 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/SigGen and TSS for FCS_COP.1/Hash.
FPT_TUD_EXT.1 (Trusted update)
Objective(s): O.UPDATE_VERIFICATION **Summary**: The TOE's firmware can be updated by an administrator by downloading a firmware bundle and installing it on the TOE. Each firmware bundle is digitally signed by HP using RSA 2048-bit and SHA2-256 algorithms. Each HCD includes a factory-installed public key from HP, which the TOE uses to verify the digital signature of the firmware bundle.

TOE SFRs and compliance rationale
An administrator can initiate a firmware update and load the firmware bundle onto the TOE through its EWS interface. Once uploaded, the TOE verifies the firmware bundle's digital signature before installation, using the RSA 2048-bit and SHA2-256 algorithms along with the factory-installed public key. If the signature verification fails, the TOE will not permit the update to proceed. The TOE uses the RSA 2048-bit and SHA2-256 algorithms in HP FutureSmart Firmware OpenSSL 1.1.1 to verify the digital signature of a firmware bundle. The RSA 2048-bit algorithm is defined in FCS_COP.1/SigGen, while the SHA2-256 hash algorithm is defined in FCS_COP.1/Hash. The [CCECG] section Updating TOE firmware describes the steps to update the TOE. The administrator can query the current version of both the System firmware and the Jetdirect Inside firmware through the Control Panel and EWS interfaces. Instructions to query the firmware versions through the EWS are provided in the [CCECG] section Check version of installed TOE firmware. **Note:** The HP Inc. Software Depot kiosk provides a SHA2-256 published hash of the firmware bundle and a Windows OS utility program that can be downloaded and used to verify the hash. Once downloaded, the firmware bundle 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.
FTA_SSL.3 (TSF-initiated termination)
Objective(s): O.USER_I&A **Summary**: This SFR applies to the interactive sessions for the Control Panel and EWS. The TOE's REST interface does not support the concept of sessions. *Control Panel* 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. *EWS* 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.
FTP_ITC.1 (Inter-TSF trusted channel)
Objective(s): O.AUDIT, O.COMMS_PROTECTION **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.

TOE SFRs and compliance rationale

The TOE provides and initiates trusted communication channels to the following authorized IT entities.

- authentication server
- DNS server
- NTS server
- SMB server
- SMTP server
- syslog server (audit server)
- WINS server

For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1.

FTP_TRP.1/Admin (Trusted path for Administrators)

Objective(s): O.COMMS_PROTECTION

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.

The following interfaces are the remote administrative interfaces of the TOE in the evaluated configuration.

- EWS (via a web browser)
- REST

For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1.

FTP_TRP.1/NonAdmin (Trusted path for Non-administrators)

Objective(s): O.COMMS_PROTECTION

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.

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.

- PJL

For more information on IPsec, see the TSS for FCS_IPSEC_EXT.1.

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES	Advanced Encryption Standard
AH	Authentication Header (IPsec)
AIA	Authority Information Access
ARM	Advanced RISC Machine
ASCII	American Standard Code for Information Interchange
BEV	Border Encryption Value
BIOS	Basic Input/Output System
CA	Certificate Authority
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
EA	Evaluation Activity
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
FQDN	Fully Qualified Domain Name
HCD	Hardcopy Device
HCDcPP	collaborative Protection Profile for Hardcopy Devices
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
LCD	Liquid-crystal Display
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
OCSP	Online Certificate Status Protocol
OSP	Organizational Security Policy
OTP	One-Time Programmable
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
SAN	Subject Alternative Name
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 Single-function Printers**

HP LaserJet Enterprise 8501

Author(s) HP Inc.

Edition 1

Date 1/2026

CCEVS-TD0926 **HIT Technical Decision: Clarification on FPT_SBT_EXT.1 Root of Trust**

Date 07/02/2025

Location https://www.niap-ccevs.org/technical-decisions/TD0926

CCEVS-TD0927 **HIT Technical Decision: Clarification on FPT_KYP_EXT.1 when using TPM-like device**

Date 07/02/2025

Location https://www.niap-ccevs.org/technical-decisions/TD0927

CCEVS-TD0928 **HIT Technical Decision: FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 Time based test case as optional**

Date 07/02/2025

Location https://www.niap-ccevs.org/technical-decisions/TD0928

CCEVS-TD0937 **CPP_HCD_V1.0 Endorsement Requirements**

Date 08/05/2025

Location https://www.niap-ccevs.org/technical-decisions/TD0937

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

HCDcPP **collaborative Protection Profile for Hardcopy Devices**

Version 1.0e

Date 4 March 2024

Location https://www.niap-ccevs.org/protectionprofiles/483

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

ISO/IEC 9797-2:2011 **Information technology — Security techniques — Message Authentication Codes (MACs)**

Version ISO/IEC 9797-2:2011

Date 2011-05

Location https://www.iso.org/standard/51618.html

KMD **Key Management Description for HP Hardcopy Devices with HP FutureSmart 5.9.2.1 Firmware and Linux 5.10**

HP LaserJet Enterprise 8501

Author(s) HP Inc.

Version 1.0

Date 2025-11-24

NIST SP 800-132 **Recommendation for Password-Based Key Derivation: Part 1: Storage Applications**

Date December 2010

Location https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

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

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-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