Swedish Certification Body for IT Security

Certification Report- HP G2 JM HCDPP

Issue: 1.0, 2022-nov-10

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is:

- HP Color LaserJet MFP E87740/E87750/E87760/E87770,
- HP Color LaserJet Flow E87740/E87750/E87760/E87770,
- HP LaserJet MFP E82650/E82660/E82670,
- HP LaserJet Flow E82650/E82660/E82670

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

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

The following firmware modules are included in the TOE:

- System firmware
- Jetdirect Inside firmware

The Security Target claims conformance to:

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

The evaluation has been performed by atsec information security AB in Danderyd, Sweden .The evaluation was completed on 2022-10-25. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm both to the evaluation activities in the HCDPP and to evaluation assurance level EAL 1, augmented by ASE_SPD.1

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

2 Identification

Certification Identification	
Certification ID	CSEC2022006
Name and version of the certified IT product	• HP Color LaserJet MFP E87740/E87750/E87760/E87770, System firmware version: 2503252_000046, Inside firmware version: JOL25030046 • HP Color LaserJet Flow E87740/E87750/E87760/E87770, System firmware version: 2503252_000046, Inside firmware version: JOL25030046 • HP LaserJet MFP E82650/E82660/E82670, System firmware version: 2503252_000042, Inside firmware version: JOL25030046 • HP LaserJet Flow E82650/E82660/E82670 System firmware version: 2503252_000042, Inside firmware version: JOL25030046
Security Target Identification	HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow E82650/E82660/E82670 Security Target, HP Inc., 2022-10-12, document version 1.6
EAL	For CCRA and EA/MLA: Protection Profile for Hardcopy Devices v1.0 as modified by Errata #1 including ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.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 For SOGIS: EAL 1 + ASE_SPD.1
Sponsor	HP Inc.
Developer	HP Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.2
Scheme Notes Release	19.0
Recognition Scope	CCRA, SOGIS and EA/MLA

Certification date	2022-11-10

3 Security Policy

The TOE provides the following security services:

- Auditing
- Data Encryption (a.k.a. cryptography)
- Identification, Authentication, and Authorization to Use HCD Functions
- Access Control
- Image Overwrite
- Trusted Communications
- Administrative Roles
- Trusted Operation
- PSTN Fax-network Separation

A brief description of each security policy is given below. A more detailed description is given in the ST.

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 IP-sec. No unauthorized access to the audit records is allowed by the TOE.

3.2 Data Encryption (a.k.a. cryptography)

3.2.1 IPsec

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

3.2.2 Drive-lock Password

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

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

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.

3.2.4 Digital Signatures for TSF Testing

The TOE uses digital signatures as part of its TSF testing functionality.

3.2.5 Cryptographic Implementations/Modules

The TOE uses multiple cryptographic implementations to accomplish its cryptographic functions. The table below provides the complete list of cryptographic implementations used to satisfy the [HCDPPv1.0] cryptographic requirements and maps the cryptographic implementations to the firmware modules.

Cryptographic implementation	Usage
HP FutureSmart Firmware OpenSSL 1.1.1	Drive-lock password (BEV) generation, TSF Testing, Trusted Update
HP FutureSmart Firmware QuickSec 7.3 Cryptographic Module	IKE
HP FutureSmart Firmware Linux Kernel Crypto API	IPsec

3.3 Identification, Authentication, and Authorization to Use HCD Functions

The following table 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.

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

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 a disk-based SED whose cryptographic functions have been CC certified. Together with the drive-lock password, the SED ensures that TSF Data and User Data on the drive is not stored as plaintext.

3.5 Image Overwrite

The TOE also supports the optional Image Overwrite function (O.IMAGE_OVERWRITE) defined in [HCDPPv1.0]. [HCDPPv1.0] limits the scope of this function to a field-replaceable nonvolatile storage device.

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

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

3.6 Trusted Communications

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

3.7 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.

3.8 Trusted Operation

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

The TOE contains TSF testing functionality referred to as Whitelisting to help ensure only authentic, known-good firmware files that have not been tampered with are loaded into memory. The TOE supports dm-verity to protect the integrity of the SquashFS file system firmware images. On each boot, the TOE verifies the digital signature of the dm-verity hash tree corresponding to a SquashFS file system firmware image. During operation, dm-verity verifies the integrity of a file system block before loading it into memory. The TOE uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to verify the integrity of a dm-verity hash tree. For additional details, see the TSS for FPT_TST_EXT.1.

3.9 PSTN Fax-network Separation

The PSTN fax capability is either included with or can be added to the TOE. In either case, the TOE provides a distinct separation between the fax capabilities and the Ethernet network connection of the TOE prohibiting communication via the fax interface except when transmitting or receiving User Data using fax protocols. This is explained in more detail along with the fax capabilities in the TSS for FDP_FXS_EXT.1.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes four assumptions on the usage and the operational environment of the TOE.

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.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

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

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.

T.UNAUTHORIZED_ACCESS - An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.

T.TSF_COMPROMISE - An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.

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

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

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

The Security Target contains seven Organisational Security Policies (OSPs), which have been considered during the evaluation.

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

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

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

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

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

P.FAX_FLOW - If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

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

5 Architectural Information

The TOE is designed to be shared by many client computers and human users. It performs the functions of printing, copying, scanning, faxing, and storing of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, to an analog telephone line using its internal analog fax modem, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration except when the administrator performs trusted update via the USB).

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

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

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.

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.

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.

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

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 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.

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

The TOE can be used to email scanned documents, email received faxes, or email sent faxes. In addition, the TOE can send email alert messages to administrator-specified email addresses, mobile devices, or to a website. The TOE supports protected communications between itself and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec to protect the communication with the SMTP gateway. The TOE can only send emails; it does not accept inbound emails.

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.

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

Each HCD contains a user interface (UI) called the Control Panel. The Control Panel consists of a touchscreen LCD, a physical home screen button, and a pull-out keyboard (“Flow” models only) as part of the Control Panel. The Control Panel is the physical interface that a user uses to communicate with the TOE when physically using the HCD. The LCD screen displays information such as menus and status to the user. It also provides virtual buttons to the user such as an alphanumeric keypad for entering usernames and passwords. Both administrative and non-administrative users can access the Control Panel.

The TOE supports both Internal Authentication mechanisms (Local Device Sign In) and External Authentication mechanisms (LDAP Sign In and Windows Sign In i.e., Kerberos).

All TOE models contain one field-replaceable nonvolatile storage device. This storage device is a disk-based self-encrypting drive (SED). It contains a section called Job Storage which is a user-visible file system where user document data, such as stored print, stored copy, and stored received faxes, are located.

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both firmware components work together to provide the security functionality of the TOE. They share the same operating system. The operating system is part of the System firmware.

6 Documentation

Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow E82650/E82660/E82670, HP Inc., Edition 1, 8/2022

7 IT Product Testing

7.1 Developer Testing

[HCDPPv1.0] does not requires the developer to perform any testing.

7.2 Evaluator Testing

The evaluator performed testing remotely by connecting to the test environment using Microsoft Remote Desktop (RDP). The developers set up the test environment with the actual TOE models in Boise, Idaho, USA. The testing was performed between 2022-05-05 and 2022-07-15 and re-testing was performed between 2022-09-15 and 2022-09-21. The tests included both automated and manual tests which the evaluator executed successfully.

The developer configured the TOE according to the [CCECG]. Before initiating the testing the evaluator verified that TOE was configured correctly. He also verified that the test environment was properly set up by the developer. The following models were tested:

TOE Name (hardware models)	Code name	System Firmware Version	Jetdirect Inside Firmware Version
Samsung Color MFP SL-X5230NR	Ammolite	2503238_000229	JOL25030046
HP Laserjet Managed Flow MFP E82650	Moonstone	2503238_000228	
Samsung Mono MFP SL-K6300	Pearl	2503238_000225	

Re-testing was performed on the same hardware models, but with the new System Firmware version:

TOE Name (hardware models)	Code name	System Firmware Version	Jetdirect Inside Firmware Version
Samsung Color MFP SL-X5230NR	Ammolite	2503251_000033	JOL25030046
HP Laserjet Managed Flow MFP E82650	Moonstone	2503251_000035	
Samsung Mono MFP SL-K6300	Pearl	2503251_000029	

The System Firmware Version was updated after testing, however no product code was updated.

The evaluator executed all required tests in [HCDPPv1.0], [ERRATA] and Technical Decisions listed in [ST] 2.1.1 "Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community ([HCDPP])".

The evaluator also re-executed 93 tests on the updated TOE version to verify that the updates to the TOE did not affect any functions of the TSF.

All test results were consistent to the expected test results.

7.3 Penetration Testing

Port scans penetration tests were performed against the TOE interfaces that are accessible to a potential attacker (IPv4 and IPv6 UDP and TCP ports of the TOE).

Since an attack requires an attack surface, the evaluator decided to start by examining if the TOE exposes such interfaces, i.e., open ports.

The TOE and operational environment was configured according to [ST] and [CCECG].

TOE Name (hardware models)	Code name	System Firmware Version	Jetdirect Inside Firmware Version
Samsung Color MFP SL-X5230NR	Ammolite	2503238_000229	JOL25030046
Samsung Mono MFP SL-K6300LX	Pearl	2503238_000225	
HP LaserJet Managed MFP E82650	Moonstone	2503238_000228	

The evaluator notes that the developer updated the System firmware to fix an issue with the seeding of OpenSSL DRBG (used for generating Drive-lock password) during the evaluation. Since the Jetdirect Inside firmware which implements the network functionality was not updated, the evaluator determined that there is no need to re-execute the port scan penetration tests on the updated firmware.

The evaluator examined all potential interfaces, i.e., all IPv4 and IPv6 UDP and TCP ports.

The evaluator examined the results from the penetration test. The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec which was the expected outcome.

8 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.
- PC Fax Send must be disabled.
- Fax polling receive must be disabled.
- Device USB must be disabled.
- Host USB plug and play must be disabled.
- Firmware upgrades through any means other than the EWS (e.g., PJL) and USB must be disabled.
- All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password.
- HP Jetdirecting XML Services must be disabled.
- External file system access through PJL and PS must be disabled.
- Only X.509v3 certificates and pre-shared key are supported methods for IPsec authentication (IPsec authentication using Kerberos is not supported).
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Mandatory Sign-in must be enabled (this disables the Guest role).
- SNMP must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to support personnel, must be disabled.
- Wireless functionality must be disabled:
  - Near Field Communication (NFC) must be disabled.
  - Bluetooth Low Energy (BLE) must be disabled.
  - Wireless Direct Print must be disabled.
  - Wireless station must be disabled.
- PJL device access commands must be disabled.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the built-in Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS) using IPsec:
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services
- Device Administrator Password must be set.
- Remote Configuration Password must not be set.
- OAUTH2 use is disallowed.
- SNMP over HTTP use is disallowed.
- HP Workpath Platform must be disabled.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- All received faxes must be converted into stored faxes.

- Fax Archive must be disabled.
- Fax Forwarding must be disabled.
- Internet Fax and LAN Fax must be disabled.
- Firmware updates through REST Web Services is disallowed.
- Scan+ must be disabled.
- Remote User Auto Capture must be disabled.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- Smart Cloud Print must be disabled.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

Assurance Class/Family		Short name	Verdict
Development		ADV	PASS
	Basic functional specification	ADV_FSP.1	PASS
Guidance Documents		AGD	PASS
	Operational User Guidance	AGD_OPE.1	PASS
	Preparative Procedures	AGD_PRE.1	PASS
	PP assurance activities	AGD_HCDPP.1	PASS
Life-cycle Support		ALC	PASS
	Labeling of the TOE	ALC_CMC.1	PASS
	TOE CM coverage	ALC_CMS.1	PASS
	PP assurance activities	ALC_HCDPP.1	PASS
Security Target Evaluation		ASE	PASS
	ST Introduction	ASE_INT.1	PASS
	Conformance Claims	ASE_CCL.1	PASS
	Security Problem Definition	ASE_SPD.1	PASS
	Security Objectives for the Operational Environment	ASE_OBJ.1	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Stated Security Requirements	ASE_REQ.1	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
	PP assurance activities	ASE_HCDPP.1	PASS
Tests		ATE	PASS
	Independent Testing - conformance	ATE_IND.1	PASS
	PP assurance activities	ATE_HCDPP.1	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability survey	AVA_VAN.1	PASS
	PP assurance activities	AVA_HCDPP.1	PASS
Entropy Description		AEN	
	PP assurance activities	AEN_HCDPP.1	PASS
Key Management Description		AKM	
	PP assurance activities	AKM_HCDPP.1	PASS

Note that the evaluators have used a notation similar to assurance classes for PP assurance activities that does not belong to a particular assurance class in CC. For PP requirements that are related to existing assurance classes, the evaluators have used a notation similar to assurance components for the requirements.

10 Evaluator Comments and Recommendations

None.

11 Glossary

AES	Advanced Encryption Standard
AH	Authentication Header (IPsec)
Arm	Advanced RISC Machine
BEV	Border Encryption Value
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Methodology for Information Technology Security
cPP	Collaborative Protection Profile
CSEC	The Swedish Certification Body for IT Security
CTR	Counter mode
CTR_DRBG	Counter mode DRBG
DH	Diffie-Hellman
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluated Assurance Level
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
FFC	Finite Field Cryptography
HCD	Hardcopy Device
HCDPP	Hardcopy Device Protection Profile
HMAC	Hashed Message Authentication Code
HP	Hewlett-Packard
I&A	Identification and Authentication
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)
ITSEF	IT Security Evaluation Facility
KAS	Key Agreement Scheme
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer

NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NTLM	Microsoft NT LAN Manager
NTS	Network Time Service
OSP	Organizational Security Policy
OXP	Open Extensibility Platform
OXPd	OXP device layer
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
RSA	Rivest-Shamir-Adleman
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
EP	External Publication
SPD	Security Problem Definition (CC)
SPI	Serial Peripheral Interface
SSC	Security Subsystem Class
ST	Security Target
TCG	Trusted Computing Group
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
USB	Universal Serial Bus
WINS	Windows Internet Name Service

12 Bibliography

ST	HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow E82650/E82660/E82670 Security Target, HP Inc., 2022-10-12, document version 1.6
HCDPPv1.0	Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP, 2015-09-10, Version 1.0
ERRATA	Protection Profile for Hardcopy Devices - v1.0, Errata #1, June 2017
CCECG	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow E82650/E82660/E82670, HP Inc., Edition 1, 8/2022
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.2	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 21 - NIAP PP Certifications
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs
- Scheme Note 25 - Use of CAVP-tests in CC evaluations
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for aplication, evalua-tion and certification