Swedish Certification Body for IT Security

Certification Report - HP G2.0 AJM BCBC HCDcPP

Issue: 1.0, 2026-feb-25

Authorisation: Hans Sharma, Junior Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the HP Color LaserJet Managed MFP E78523/E78528/E78530, HP Color LaserJet Managed MFP E87740/E87750/E87760/E87770, HP Color LaserJet Managed Flow MFP E87740/ E87750/E87760/E87770, HP Color LaserJet Enterprise MFP 8801, HP Color LaserJet Enterprise Flow MFP 8801, HP LaserJet Managed MFP E82650/E82660/E82670, HP LaserJet Managed Flow MFP E82650/E82660/E82670, HP LaserJet Enterprise MFP 8601, HP LaserJet Enterprise Flow MFP 8601, HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, HP Color LaserJet Managed MFP E47528, HP Color LaserJet MFP 6800, HP Color LaserJet Flow MFP 6800/6801, HP Color LaserJet MFP X67755/X67765, HP Color LaserJet Flow MFP X67755/X67765, HP Color LaserJet MFP 5800, HP Color LaserJet Flow MFP 5800, HP Color LaserJet MFP X57945, HP Color LaserJet Flow MFP X57945, HP Color LaserJet MFP X58045, and HP Color LaserJet Flow MFP X58045 printers with HP FutureSmart 5.9.2.1 Firmware. The TOE type is a hardcopy device (HCD) also known as a multifunction printer (MFP).

The following firmware modules are included in the TOE:

• System firmware

• Jetdirect Inside firmware

The ST claims exact conformance to the collaborative Protection Profile for Hardcopy Devices, Version 1.0e, dated 4 March 2024 (HCDcPP).

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden.

The evaluation was completed on 2026-02-17. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 revision 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 the security claims in the Security Target (ST) and the collaborative Protection Profile for Hardcopy Devices.

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.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2025006
Name and version of the certified IT product	HP G2.0 AJM BCBC HCDcPP
Security Target Identification	HP Color LaserJet Managed MFP E78523/E78528/E78530, HP Color LaserJet Managed MFP E87740/E87750/E87760/E87770, HP Color LaserJet Managed Flow MFP E87740/ E87750/E87760/E87770, HP Color LaserJet Enterprise MFP 8801, HP Color LaserJet Enterprise Flow MFP 8801, HP LaserJet Managed MFP E82650/E82660/E82670, HP LaserJet Managed Flow MFP E82650/E82660/E82670, HP LaserJet Enterprise MFP 8601, HP LaserJet Enterprise Flow MFP 8601, HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, HP Color LaserJet Managed MFP E47528, HP Color LaserJet MFP 6800, HP Color LaserJet Flow MFP 6800/6801, HP Color LaserJet MFP X67755/X67765, HP Color LaserJet Flow MFP X67755/X67765, HP Color LaserJet MFP 5800, HP Color LaserJet Flow MFP 5800, HP Color LaserJet MFP X57945, HP Color LaserJet Flow MFP X57945, HP Color LaserJet MFP X58045, HP Color LaserJet Flow MFP X58045, Security Target, HP Inc., document version 1.11
EAL	HCDcPP
Sponsor	HP Inc.
Developer	HP Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	QMS 2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026-02-26

3 Security Policy

The major security functions of the TOE are as follows:

- Identification, authentication, and authorization to use HCD functions
- Access control
- Encryption
- Trusted communications
- Administrative roles
- Auditing
- Trusted operation
- PSTN fax-network separation (if PSTN fax function is present)

3.1 Identification, Authentication, and Authorization to Use HCD Functions

The Local Device Sign In method uses an internal user account database to authenticate users. The user accounts contain the user attributes Display name and Password, which are used for identification and authentication (I&A). Although this method supports multiple accounts, only the built-in Device Administrator account (U.ADMIN) is to be used with this method in the evaluated configuration. The administrator must not create any Local Device Sign In accounts.

External authentication is handled via LDAP or Windows 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.

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.

More in-depth information can be found in the ST.

3.2 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 permission sets (PS) 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 HDD, SSD, or eMMC. The TSF ensures that confidential TSF Data and User Document Data stored on the drive is not stored as plaintext.

3.3 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.

3.4 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.

3.5 Trusted Operation

TOE firmware bundles can be downloaded from the HP Inc. website to update the TOE’s firmware. These bundles 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.

3.6 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

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.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.

4.1 Clarification of Scope

The Security Target contains six 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 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.

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 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

P.FAX_FLOW

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

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.

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/retrieving of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, to an analog telephone line using its internal analog fax modem, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration except when the administrator performs trusted update via the USB). 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.

The TOE's operating system is Linux 5.10 running on an ARM Cortex-A72 processor.

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).

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

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 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.

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

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.

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 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.

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 the servers over an IPsec connection.

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.

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.

All TOE models contain one field-replaceable nonvolatile storage device. This storage device is a self-encrypting Hard Disk Drive (HDD), Solid State Drive (SSD) or eMMC. The drive contains a section called Job Storage which is a user-visible file system where user document data, such as stored print, stored copy, and stored received faxes, are located.

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, IPsec, and contains the HP FutureSmart Firmware Linux Kernel Crypto API which implements cryptographic algorithms relied upon by TOE security functionality (i.e., IPsec).

6 Documentation

Common Criteria Evaluated Configuration Guide for HP Multifunction Printers
HP Color LaserJet Managed MFP E78523/E78528/E78530,
HP Color LaserJet Managed MFP E87740/E87750/E87760/E87770,
HP Color LaserJet Managed Flow MFP E87740/ E87750/E87760/E87770,
HP Color LaserJet Enterprise MFP 8801,
HP Color LaserJet Enterprise Flow MFP 8801,
HP LaserJet Managed MFP E82650/E82660/E82670,
HP LaserJet Managed Flow MFP E82650/E82660/E82670,
HP LaserJet Enterprise MFP 8601,
HP LaserJet Enterprise Flow MFP 8601,
HP LaserJet Enterprise MFP M430/M431,
HP Color LaserJet Enterprise MFP M480,
HP LaserJet Managed MFP E42540,
HP Color LaserJet Managed MFP E47528,
HP Color LaserJet MFP 6800,
HP Color LaserJet Flow MFP 6800/6801,
HP Color LaserJet MFP X67755/X67765,
HP Color LaserJet Flow MFP X67755/X67765,
HP Color LaserJet MFP 5800,
HP Color LaserJet Flow MFP 5800,
HP Color LaserJet MFP X57945,
HP Color LaserJet Flow MFP X57945,
HP Color LaserJet MFP X58045,
HP Color LaserJet Flow MFP X58045
Edition 1, 1/2026

7 IT Product Testing

7.1 Developer Testing

[CPP_HCD_V1.0E] does not require 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 setup the test environment with the actual TOE models in Boise, Idaho, USA. The testing was performed between 2025-10-13 and 2025-11-26. The tests included both automated and manual tests which the evaluator executed successfully.

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

The following models were tested:

TOE Name (hardware models)	System Firmware Version	Jetdirect Inside Firmare Version
HP Color Laserjet MPF M480	2509306_000329	JOL25090252
HP Color Laserjet Flow 5800	2509306_000319	JOL25090252
HP Color Laserjet Flow E87740	2509306_000318	JOL25090252

7.3 Penetration Testing

Port scans penetration tests were performed against the TOE interfaces that are accessible to a potential attacker (IPv4 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)	System Firmware Version	Jetdirect Inside Firmare Version
HP Color Laserjet MPF M480	2509306_000329	2509306_000318
HP Color Laserjet Flow 5800	2509306_000319	2509306_000318
HP Color Laserjet Flow E87740	2509306_000318	2509306_000318

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

The evaluator examined the results from the penetration test and provided a summary within the [EPT] "Evaluator penetration testing AJM BCBC HCDcPP". The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec which was the expected outcome.

8 Evaluated Configuration

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.

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

• HP Digital Sending Software (DSS) must be disabled.

• Only one Administrative Computer is used to manage the TOE.

• Third-party solutions must not be installed on the TOE.

• PC Fax Send must be disabled.

• Fax polling receive must be disabled.

• Device USB must be disabled.

• Host USB plug and play must be disabled.

• Firmware upgrades through any means other than the EWS (e.g., PJL) and USB must be disabled.

• All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password.

• HP Jetdirect XML Services must be disabled.

• External file system access through PJL and PS must be disabled.

• Only X.509v3 certificates 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.

- All received faxes must be converted into stored faxes.
- Fax Archive must be disabled.
- Fax Forwarding must be disabled.
- Internet Fax and LAN Fax must be disabled.
- Firmware updates through REST Web Services is disallowed.
- Remote User Auto Capture must be disabled.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- 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 non-fax jobs must be assigned a Job PIN or Job Encryption Password

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 [1] <e.g. 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.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family		Short name	Verdict
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	ASE_OBJ.1	PASS
	Extemnded Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.1	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
	HCcPP assurance activities	ASE_HCDCPP.1	PASS
Development		ADV	PASS
	Functional Specification	ADV_FSP.1	PASS
	HCcPP assurance activities	ADV_HCDCPP.1	PASS
Guidance documents		AGD	PASS
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
	HCcPP assurance activities	AGD_HCDCPP.1	PASS
Life-cycle Support		ALC	PASS
	CM Capabilities	ALC_CMC.1	PASS
	CM Scope	ALC_CMS.1	PASS
Tests		ATE	PASS
	Independent Testing	ATE_IND.	PASS
	HCcPP assurance activities	ATE_HCDCPP.1	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.1	PASS
	HCcPP assurance activities	AVA_HCDCPP.1	PASS

[1] State the level of attack potential that is applicable.

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

12 Bibliography

ST	HP Color LaserJet Managed MFP E78523/E78528/E78530, HP Color LaserJet Managed MFP E87740/E87750/E87760/E87770, HP Color LaserJet Managed Flow MFP E87740/ E87750/E87760/E87770, HP Color LaserJet Enterprise MFP 8801, HP Color LaserJet Enterprise Flow MFP 8801, HP LaserJet Managed MFP E82650/E82660/E82670, HP LaserJet Managed Flow MFP E82650/E82660/E82670, HP LaserJet Enterprise MFP 8601, HP LaserJet Enterprise Flow MFP 8601, HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, HP Color LaserJet Managed MFP E47528, HP Color LaserJet MFP 6800, HP Color LaserJet Flow MFP 6800/6801, HP Color LaserJet MFP X67755/X67765, HP Color LaserJet Flow MFP X67755/X67765, HP Color LaserJet MFP 5800, HP Color LaserJet Flow MFP 5800, HP Color LaserJet MFP X57945, HP Color LaserJet Flow MFP X57945, HP Color LaserJet MFP X58045, HP Color LaserJet Flow MFP X58045, Security Target, HP Inc., document version 1.11
CPP_HCD_V1.0e	Collaborative Protection Profile for Hardcopy Devices, 2024-03-04, version 1.0e
CCECG	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP Color LaserJet Managed MFP E78523/E78528/E78530, HP Color LaserJet Managed MFP E87740/E87750/E87760/E87770, HP Color LaserJet Managed Flow MFP E87740/ E87750/E87760/E87770, HP Color LaserJet Enterprise MFP 8801, HP Color LaserJet Enterprise Flow MFP 8801, HP LaserJet Managed MFP E82650/E82660/E82670, HP LaserJet Managed Flow MFP E82650/E82660/E82670, HP LaserJet Enterprise MFP 8601, HP LaserJet Enterprise Flow MFP 8601, HP LaserJet Enterprise MFP M430/M431, HP Color LaserJet Enterprise MFP M480, HP LaserJet Managed MFP E42540, HP Color LaserJet Managed MFP E47528, HP Color LaserJet MFP 6800, HP Color LaserJet Flow MFP 6800/6801, HP Color LaserJet MFP X67755/X67765,

	HP Color LaserJet Flow MFP X67755/X67765, HP Color LaserJet MFP 5800, HP Color LaserJet Flow MFP 5800, HP Color LaserJet MFP X57945, HP Color LaserJet Flow MFP X57945, HP Color LaserJet MFP X58045, HP Color LaserJet Flow MFP X58045
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	Common Criteria v.3.1 revision 5
CEM	mon Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

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
2.6.1	2025-10-16	None
2.6	2025-03-17	None
2.5.2	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 22 - Vulnerability assessment
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for aplication, evaluation ad certification
- Scheme Note 30 - CM of third party components