Swedish Certification Body for IT Security

Certification Report - HP G2.0 BC 2600PP

Issue: 1.0, 2024-jun-11

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the HP FutureSmart 5.6.0.2 Firmware for the

HP LaserJet MFP E78523/E78528, HP LaserJet MFP E73025/E73030, HP Color LaserJet MFP E78625/E78630/E78635, HP Color LaserJet Flow MFP E78625/E78630/E78635, HP LaserJet MFP E73130/E73135/E73140, HP LaserJet Flow MFP E73130/E73135/E73140, HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow MFP E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow MFP E82650/E82660/E82670, 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 multi-function printers.

The TOE is the contents of the firmware and the operating system. The operating system is Linux 4.9.230. The following firmware modules are included in the TOE:

- System firmware
- Jetdirect Inside firmware

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.

The consumer receives the hardware independent of the ZIP file. The evaluated hardware models are either already on the consumer's premises or must be obtained from HP Inc.

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

- [PP2600.1]: IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A". Version 1.0 as of June 2009; demonstrable conformance.

- [PP2600.1-CPY]: SFR Package for Hardcopy Device Copy Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-DSR]: SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-FAX]: SFR Package for Hardcopy Device Fax Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-PRT]: SFR Package for Hardcopy Device Print Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-SCN]: SFR Package for Hardcopy Device Scan Functions. Version 1.0 as of June 2009; demonstrable conformance.
- [PP2600.1-SMI]: SFR Package for Hardcopy Device Shared-medium Interface Functions. Version 1.0 as of June 2009; demonstrable conformance.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden. A virtual Site-visit was performed Boise, Idaho, USA.

The evaluation was completed on 2024-05-22. 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, and by observing site-visit. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 3 augmented by ALC_FLR.2.

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	CSEC2022013
Name and version of the certified IT product	• HP Color LaserJet MFP E78523/E78528 System firmware version: 2506649_040425 Inside firmware version: JOL25060606 • HP LaserJet MFP E73025/E73030 System firmware version: 2506649_040435 Inside firmware version: JOL25060606 • HP Color LaserJet MFP E78625/E78630/E78635, HP Color LaserJet Flow MFP E78625/E78630/E78635 System firmware version: 2506649_040420 Inside firmware version: JOL25060606 • HP LaserJet MFP E73130/E73135/E73140, HP LaserJet Flow MFP E73130/E73135/E73140 System firmware version: 2506649_040417 Inside firmware version: JOL25060606 • HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow MFP E87740/E87750/E87760/E87770 System firmware version: 2506649_040426 Inside firmware version: JOL25060606 • HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow MFP E82650/E82660/E82670 System firmware version: 2506649_040423 Inside firmware version: JOL25060606 • HP Color LaserJet MFP 6800, HP Color LaserJet Flow MFP 6800, HP Color LaserJet Flow MFP 6801, HP Color LaserJet MFP X67755/X67765, HP Color LaserJet Flow MFP X67755/X67765 System firmware version: 2506649_040449 Inside firmware version: JOL25060606 • HP Color LaserJet MFP 5800, HP Color LaserJet Flow MFP 5800, HP Color LaserJet MFP X57945/X58045, HP Color LaserJet Flow MFP X57945/ X58045 System firmware version: 2506649_040428 Inside firmware version: JOL25060606 •
Security Target Identification	HP LaserJet MFP E78523/E78528, HP LaserJet MFP E73025/E73030, HP Color LaserJet MFP E78625/E78630/E78635, HP Color LaserJet Flow MFP E78625/E78630/E78635, HP LaserJet MFP E73130/E73135/E73140,

	HP LaserJet Flow MFP E73130/E73135/E73140, HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow MFP E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow MFP E82650/E82660/E82670, 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., 2024-01-25, document version 1.0.
EAL	EAL 3 + ALC_FLR.2
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	2.5.1
Scheme Notes Release	21.0
Recognition Scope	CCRA, EA/MLA
Certification date	2024-06-11

3 Security Policy

- Auditing
- Cryptography
- Identification and Authentication
- Data Protection and Access Control
- Protection of the TSF
- TOE Access Protection
- Trusted Channel Communication and Certificate Management
- User and Access Management

3.1 Auditing

The TOE performs auditing of security-relevant functions. The TOE connects and sends audit records to a syslog server (part of the Operational Environment) for long-term storage and audit review. 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.

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library is used to supply the cryptographic algorithms for IKE, and the Linux Kernel Crypto API is used to supply the cryptographic algorithms for IPsec.

The TOE supports the decrypting of an encrypted stored print job. To decrypt an encrypted stored print job, the TOE derives a key from a Job Encryption Password and unlocks the decryption key using the derived key. The TOE then decrypts the encrypted stored print job using the decryption key.

The TOE's on-demand Data Integrity Test and Code Integrity Test use the SHA-256 algorithm to verify the integrity of TSF Data and TOE executable code, respectively. The OpenSSL 1.1.1n library within the TOE supplies the SHA2-256 algorithm.

3.3 Identification and Authentication

The TOE supports multiple Control Panel sign in methods, both local and remote methods:

- Local sign in method:
  - Local Device Sign In (Local Administrator account only)
- Remote sign in methods:
  - LDAP Sign In
  - Windows Sign In (via Kerberos)

The Control Panel allows both non-administrative users (U.NORMAL) and administrative users (U.ADMINISTRATOR) to sign in.

The TOE also uses IPsec to identify and mutually authenticate the

following user types:

- Administrative Computer (U.ADMINISTRATOR)
- Network Client Computers (U.NORMAL)

3.4 Data Protection and Access Control

- Permission Sets - For Control Panel users, the TOE uses a user's User Role (as determined by each user's Permission Set) to determine a user's access to many TOE functions. Only U.ADMINISTRATOR can query, create, modify, and delete Permission Sets. In addition, only U.ADMINISTRATOR can query, create, modify, and delete the Permission Set associations to users.
- Job PINs - Users can control access to each stored print and stored copy job that they place under the TOE's control by assigning a Job PIN to each job. A Job PIN limits access to a stored print or stored copy job while the job resides under the TOE's control and allows a user to control when the job is printed so that physical access to the hard copies can be controlled by the user. A Job PIN must be 4 digits.
- Job Encryption Passwords - The TOE can store and decrypt encrypted stored print jobs received from a client computer. To decrypt the encrypted stored print job at the Control Panel, a user must enter the correct Job Encryption Password that was used to derive the key to protect the job.
- Common access control - The TOE protects each non-fax job in Job Storage from non-administrative users through the use of a user identifier and a Job PIN or through the use of a Job Encryption Password. The TOE protects each fax job in Job Storage through the Permission Set mechanism. A user must have a specific fax permission in their Permission Set to access received fax jobs stored in Job Storage. Scan jobs are ephemeral and not stored in Job Storage. Only the user performing the scan can access the job on the TOE.
- TOE function access control - The TOE controls access to TOE functions available at the Control Panel using permissions defined in Permission Sets. During the Control Panel sign-in process, the TOE authorizes the user after they are successfully identified and authenticated. As part of the user authorization process, the TOE associates Permission Sets to the user and then applies a Permission Set (which is the combination of the Permission Sets associated to the user). The applied Permission Set (a.k.a. session Permission Set) becomes the user's User Role. Control Panel applications (e.g., Copy, Fax, Print from Job Storage) use the user's session Permission Set to determine which of the application's functions should be allowed or disallowed for the user.
  For IPsec users, the TOE uses the IPsec to control access to the supported network service protocols. The IPsec contains the IP addresses of authorized client computers grouped into address templates and the network service protocols grouped into service templates. The administrator maps an address template to a service template using an IPsec rule.
  Service templates, therefore, act as the User Roles for IPsec users. IP addresses of computers not contained in a rule are denied access to the TOE.
- Residual information protection - When the TOE deletes an object, the contents of the object are no longer available to TOE users. This prevents TOE users from attempting to recover deleted objects of other users via the TOE interfaces.

3.5 Protection of the TSF

- Restricted forwarding of data to external interfaces (including fax separation) - The TOE does not allow forwarding of data to an External Interface. The TOE contains only one External Interface in the evaluated configuration and that interface is the Shared-medium Interface. The analog fax hardware and the firmware that controls the fax hardware do not have the ability to access the Shared-medium fax functions. No pathway is provided to the Shared-medium interface from the fax.
- TSF self-testing - The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of TSF functional tests (including system clock verification, LDAP settings verification, and Windows settings verification), TSF data integrity tests, and TSF code integrity tests.
- Reliable timestamps - The TOE contains a system clock that is used to generate reliable timestamps. In the evaluated configuration, the administrator must configure the TOE to synchronize its system clock with a Network Time Protocol (NTP) server.

3.6 TOE Access Protection

- Inactivity timeout - The TOE supports an inactivity timeout for Control Panel sign-in sessions. If a signed-in user is inactive for longer than the specified period of inactivity, the user is automatically signed out of the Control Panel by the TOE. The inactivity period is managed by the administrator through EWS (HTTP) or the Control Panel.

3.7 Trusted Channel Communication and Certificate Management

Shared-medium communications (i.e., Ethernet) between the TOE and other trusted IT products use a trusted channel mechanism to protect the communications from disclosure and modification. The TOE also ensures the cryptographic operations are validated during policy processing such as validating digital signatures or encrypting and decrypting data. IPsec with X.509v3 certificates is used to provide the trusted communication channels. The EWS (HTTP) allows administrators to manage X.509v3 certificates used by IPsec.

3.8 User and Access Management

The TOE supports the following roles:

- Administrators (U.ADMINISTRATOR)
- Users (U.NORMAL)

Administrators maintain and configure the TOE and Operational Environment. Users perform the standard print, copy, fax, etc. functions on the system.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.USER.TRAINING

TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

A.ADMIN.TRAINING

Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. The organization security policies and procedures include security awareness training covering topics such as how to identify and avoid clicking on malicious links.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

4.2 Environmental Assumptions

The Security Target [ST] makes five assumptions on the operational environment of the TOE.

A.ACCESS.MANAGED

The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

A.ADMIN.PC.SECURE

The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it.

A.USER.PC.POLICY

User computers are configured and used in conformance with the organization's security policies

A.SERVICES.RELIABLE

When the TOE uses any of the network services DNS, FTP, Kerberos, LDAP, NTP, SMTP, syslog, SMB, SharePoint, and/or WINS, these services provide reliable information and responses to the TOE.

A.EMAILS.PROTECTED

For emails received by the SMTP gateway from the TOE, the transmission of emails between the SMTP gateway and the email’s destination is protected.

4.3 Clarification of Scope

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

T.DOC.DIS

User Document Data may be disclosed to unauthorized persons.

T.DOC.ALT

User Document Data may be altered by unauthorized persons.

T.FUNC.ALT

User Function Data may be altered by unauthorized persons.

T.PROT.ALT

TSF Protected Data may be altered by unauthorized persons.

T.CONF.DIS

TSF Confidential Data may be disclosed to unauthorized persons.

T.CONF.ALT

TSF Confidential Data may be altered by unauthorized persons.

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

P.USER.AUTHORIZATION

To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION

To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING

To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT

To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

P.ADMIN.PASSWORD

To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that it is required to perform security-relevant actions through the EWS (HTTP), REST (HTTP), and Control Panel interfaces.

P.USERNAME.CHARACTER_SET

To prevent ambiguous user names in the TOE's audit trail, the user names of the LDAP and Windows Sign In users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

P.REMOTE_PANEL.DISALLOWED

To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature

5 Architectural Information

The TOE is the firmware of an MFP designed to be shared by many client computers and human users. It performs the functions of printing, copying, scanning, faxing, storing, and retrieving of documents. It can be connected to a wired local network through the embedded Jetdirect Inside print server'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).

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

The REST Web Services interface allow administrators to externally manage the TOE over HTTP. This interface is protected using IPsec.

Printer Job Language (PJL) is used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL 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 protects all non-broadcast/non-multicast network communications with IPsec. Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using X.509v3 certificates. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) into the TOE along with the CA certificate.

Because IPsec authenticates the computers (not the individual users of the computer), access to the Administrative Computer should be restricted to TOE administrators only.

The TOE distinguishes between the Administrative Computer and Network Client Computers by using IP addresses, and IPsec. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one and the Device Administrator Password must be set.

Network Client Computers connect to the TOE using IPsec with X.509v3 certificates to protect the communication and to mutually authenticate. These client computers can send print jobs to the TOE using the PJL interface as well as receive job status.

The TOE supports an optional analog telephone line connection for sending and receiving faxes. The Control Panel uses identification and authentication to control access for sending analog faxes.

The TOE protects stored non-fax jobs with either a 4-digit Job PIN or by accepting (and storing) an encrypted print job from a client computer. Both protection mechanisms are optional by default and are mutually exclusive of each other if used. In the evaluated configuration, all stored non-fax jobs must either be assigned a 4-digit Job PIN or be an encrypted print job.

The TOE also supports Microsoft SharePoint and remote file systems for the storing of scanned documents. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to SharePoint and the remote file systems. For remote file system connectivity, the TOE supports the FTP and SMB protocols.

The TOE can be used to email scanned documents. In addition, the TOE can send email alert messages to administrator-specified email addresses, or send automated emails regarding product configuration and MFP supplies to HP. The TOE supports protected communications between itself and SMTP gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate with the SMTP gateway. The TOE can only protect unencrypted emails 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 name resolution using the DNS and WINS. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to the name resolution servers.

The TOE automatically synchronizes its system clock with an NTP server. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to the NTP server.

Each HCD contains a user interface called the Control Panel. The Control Panel 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 both Local sign-in method (Local Device Sign In) and Remote sign-in methods (LDAP Sign In and Windows Sign In).

The TOE supports the auditing of document-processing functions and security-relevant events by generating and forwarding audit records to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between itself and the syslog server and for mutual authentication of both endpoints.

6 Documentation

Common Criteria Evaluated Configuration Guide for HP Multi-function Printers HP LaserJet MFP E78523/E78528, HP LaserJet MFP E73025/E73030, HP Color LaserJet MFP E78625/E78630/E78635, HP Color LaserJet Flow MFP E78625/E78630/E78635, HP LaserJet MFP E73130/E73135/E73140, HP LaserJet Flow MFP E73130/E73135/E73140, HP Color LaserJet MFP E87740/E87750/E87760/E87770, HP Color LaserJet Flow MFP E87740/ E87750/E87760/E87770, HP LaserJet MFP E82650/E82660/E82670, HP LaserJet Flow MFP E82650/E82660/E82670, 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, 2/2024	[CCECG]

7 IT Product Testing

7.1 Developer Testing

Testing was performed by the developer at the HP site in Boise, Idaho, USA.

The approach for testing was to provide at least one test case for each Security Functional Requirement mapped to the TOE security functionality documented.

The developer reported that all tests were completed successfully, and the evaluator has examined the test evidence and verified that the test results for the manual and automated tests were consistent and clearly identify the outcome of the test action.

7.2 Evaluator Testing

The evaluator has re-run all automated tests, and a sample of manual tests. This included both regular and IPsec tests. The evaluator executed 2 regular manual tests, 4 manual IPsec tests and all the 76 automated developer tests. The evaluator did not perform any additional tests as the existing tests, both manual and automated covered all the interfaces.

Testing was performed on the following models of the TOE:

TOE Name (hardware Models)	System Firmware Version	Jetdirect Inside Firmware Version
HP Color LaserJet Enterprise MFP 6800	2506649_040449	JOL25060606
HP Color LaserJet Flow 5800	2506649_040428	JOL25060606
HP Color LaserJet MFP E78523	2506649_040425	JOL25060606

The evaluator chose to perform manual IPsec tests on Citrine (Samsung) TOE model (CSEC2023012) which also uses Jetdirect Inside Firmware Version JOL25060606 where IPsec implementation is located. Please see the Samsung evaluation (CSEC2023012) for more details on IPsec testing performed.

All tests performed by the evaluator were completed successfully.

7.3 Penetration Testing

Penetration testing was performed against the TOE interfaces that are accessible to a potential attacker. I.e., the IPv4 and IPv6 TCP and UDP 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 and available services.

The following TOE models were tested during penetration testing:

TOE Name (hardware Models)	System Firmware Version	Jetdirect Inside Firmware Version
HP Color LaserJet Enterprise MFP 6800	2506649_040449	JOL25060606

HP Color LaserJet Flow 5800	2506649_040428	JOL25060606
HP Color LaserJet MFP E78523	2506649_040425	JOL25060606

The evaluator examined the externally accessible interfaces (UDP and TCP ports), i.e., all IPv4 and IPv6 UDP and TCP ports.

The results of the port scan indicate that no attack surface is present.

8 Evaluated Configuration

The following components are required as part of the Operational Environment:

- The applicable MFP model for running the TOE firmware
- Domain Name System (DNS) server
- One administrative client computer connected to the TOE in the role of an Administrative Computer. It must contain:
  - Web browser
- One or both of the following:
  - Lightweight Directory Access Protocol (LDAP) server
  - Windows domain controller/Kerberos server
- Syslog server
- Windows Internet Name Service (WINS) server
- Network Time Protocol (NTP) server

The following components are optional in the Operational Environment:

- Client computers connected to the TOE in a non-administrative computer role
- The HP Universal Print Driver for client computers (for submitting print job requests fromclient computers)
- Simple Mail Transfer Protocol (SMTP) gateway
- Microsoft SharePoint
- Remote file systems:
  - File Transfer Protocol (FTP)
  - Server Message Block (SMB)

In the evaluated configuration the following requirements must be met:

- 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 and Host USB plug and play must be disabled.
- Firmware upgrades sent as print jobs through P9100 interface must be disabled.
- All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password.
- Jetdirect XML Services must be disabled.
- External file system access through PJL and PS must be disabled.
- IPsec authentication using X.509v3 certificates must be enabled (IPsec authentication using Kerberos or Pre-Shared Key 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 HP 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.
- User names for the LDAP and Windows Sign In users must only contain the characters defined in P.USERNAME.CHARACTER_SET.
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.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 the Jetdirect Inside's IPsec Policy:
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services
- Device Administrator Password must be set as per P.ADMIN.PASSWORD.
- 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.

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

Assurance Class Name / Assurance Family Name	*Short name*	*Verdict*
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Functional specification with complete summary	ADV_FSP.3	PASS
Architectural design	ADV_TDS.2	PASS
Guidance documents	AGD:	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC:	PASS
Authorisation controls	ALC_CMC.3	PASS
Implementation representation CM coverage	ALC_CMS.3	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Security Target evaluation	ASE:	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE:	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS

Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA:	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

Based on the assessments in the AVA report, the evaluator determined that there are no exploitable vulnerabilities in the TOE for attack potential basic. However, the evaluator identified one residual vulnerability (CVE-2024-0794).

11 Bibliography

ST
HP LaserJet MFP E78523/E78528,
HP LaserJet MFP E73025/E73030,
HP Color LaserJet MFP E78625/E78630/E78635,
HP Color LaserJet Flow MFP E78625/E78630/E78635,
HP LaserJet MFP E73130/E73135/E73140,
HP LaserJet Flow MFP E73130/E73135/E73140,
HP Color LaserJet MFP E87740/E87750/E87760/E87770,
HP Color LaserJet Flow MFP E87740/ E87750/E87760/E87770,
HP LaserJet MFP E82650/E82660/E82670,
HP LaserJet Flow MFP E82650/E82660/E82670,
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., 2024-01-25, document version 1.0

PP2600A
2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, IEEE Computer Society, 12 June 2009, version 1.0

CCECG
Common Criteria Evaluated Configuration Guide for HP Multi-function Printers
HP LaserJet MFP E78523/E78528,
HP LaserJet MFP E73025/E73030,
HP Color LaserJet MFP E78625/E78630/E78635,
HP Color LaserJet Flow MFP E78625/E78630/E78635,
HP LaserJet MFP E73130/E73135/E73140,
HP LaserJet Flow MFP E73130/E73135/E73140,
HP Color LaserJet MFP E87740/E87750/E87760/E87770,
HP Color LaserJet Flow MFP E87740/ E87750/E87760/E87770,
HP LaserJet MFP E82650/E82660/E82670,
HP LaserJet Flow MFP E82650/E82660/E82670,
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, 2/2024

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
CEM	Common 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
2.5	2024-01-25	None
2.4.2	2023-09-20	None
2.4.1	2023-09-14	None
2.4	2023-06-15	None
2.3.1	2023-04-20	None
2.3	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 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 application, evaluation and certification
- Scheme Note 31 - New procedures for site visit oversight and testing oversight