Swedish Certification Body for IT Security

Certification Report - HP CJA 2600PP

Issue: 1.0, 2022-mar-02

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is HP FutureSmart 4.11.0.1 Firmware for the HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725, and HP PageWide Enterprise Color MFP 586 multifunction printers with the following elements:

- HP FutureSmart 4.11.0.1 Firmware
- Guidance documentation

The TOE is the contents of the firmware with the exception of the operating system which is part of the Operational Environment. The following firmware modules are included in the TOE:

- System firmware
- Jetdirect Inside firmware

The firmware and guidance documentation are packaged in a single ZIP file and available for download from the HP Inc. website. The firmware is packaged in this ZIP file as a single firmware bundle. This firmware bundle contains the HP FutureSmart firmware, which in turn contains the System firmware and Jetdirect Inside firmware.

In order to download the ZIP file, the customer needs to register with HP and sign into a secure website (HTTPS) to access the download page. The customer can receive sign-in credentials by sending an email to ccc-hp-enterprise-imaging-printing@hp.com. On the download site, a SHA-256 checksum is provided along with instructions on how to use it for verification of the integrity of the downloaded package.

The 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. The evaluation was completed on 2022-02-11.

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 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.

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.

As specified in the security target of this evaluation, the implementation of some cryptographic primitives has been located in TOE environment, while the invocation of those primitives has been included in the TOE. Therefore the invocation of those primitives has been in the scope of this evaluation, while correctness of implementation of those primitives has been excluded from the TOE. Correctness of implementation is done through third party certification Cryptographic Algorithm Validation Program (CAVP) certificate SHS #4474 referred to in table 49 in the Security Target. Users of this product are advised to consider their acceptance of this third party affirmation regarding the correctness of implementation of the cryptographic primitive.

2 Identification

Certification Identification	
Certification ID	CSEC2020021
Name and version of the certified IT product	HP FutureSmart 4.11.0.1 Firmware for the HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330 HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725 and HP PageWide Enterprise Color MFP 586. See table 1 in the [ST] for the exact model names and firmware versions.
Security Target Identification	HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725, HP PageWide Enterprise Color MFP 586 Security Target
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	2.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2022-03-02

3 Security Policy

The primary security features of the TOE are:

• 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 document-processing functions and security-relevant events. Both the Jetdirect Inside and HCD System firmware generate audit records. The TOE connects and sends audit records to a syslog server for long-term storage and audit review. (The syslog server is part of the Operational Environment.)

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The HP FutureSmart QuickSec 5.1 (a.k.a. QuickSec) cryptographic library within the TOE is used to supply the cryptographic algorithms for IPsec. The TOE supports key derivation and decryption for printing encrypted stored print jobs. Both the key derivation function and decryption algorithm used by the TOE for this are included in the TOE.

The TOE contains a Data Integrity Test that provides administrators the ability to verify the integrity of specific TSF Data TOE on-demand through the EWS. The Data Integrity Test uses the SHA-256 algorithm to verify the integrity of TSF Data. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA-256 algorithm.

The TOE contains a Code Integrity Test that provides administrators the ability to verify the integrity of TOE executable code files stored on the storage drive on-demand through the EWS. The Code Integrity Test uses the SHA-256 algorithm to verify the integrity of TOE executable code files. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA-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 control access to print jobs that they place in Job Storage by assigning Job PINs to these jobs (required in the evaluated configuration). Job PINs must be 4 digits in length. Job PINs limit access to these jobs while they reside on the TOE and allow users to control when the jobs are printed so that physical access to the hard copies can be controlled.
- 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 print 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. Every print job in Job Storage is assigned either a Job PIN or a Job Encryption Password by the user at job creation time. If the TOE receives a print job from a client computer without either a Job PIN or a Job Encryption Password, the TOE cancels the job.
- TOE function access control - For Control Panel users, the TOE controls access to Control Panel applications (e.g., Print from Job Storage) using Permission Sets and, optionally, sign-in methods (authentication databases). Permission Sets act as User Roles to determine if the user can perform a function controlled by permissions.
- Each Control Panel application requires the user to have one or more specific permissions in their session Permission Set in order to access that application. In addition, the TOE's administrator can map a sign-in method to each Control Panel application and require the user to be authenticated to that sign-in method in order to access that application. The individual applications only check and enforce permissions. They do not check the sign-in methods. Instead, the TOE enforces the sign-in method requirement at the time that the user signs in to the TOE by removing permissions from the user's session Permission Set for each application in which the user's sign-in method does not match the sign-in method required by the TOE. By removing the permissions required by each non-matching application, the TOE limits the set of applications that the user can access.

  Administrators can change/modify the sign-in method mapped to each application. In addition, the TOE contains a function that allows administrators to select if the sign-in method application mappings are enforced or ignored by the TOE. This function is called "Allow users to choose alternate sign-in methods at the product control panel." When this function is disabled, the TOE enforces the "sign-in method to application" mappings and prunes (reduces) the user's session Permission Set accordingly. When this function is enabled, the sign-in method mappings are ignored by the TOE and the user's session Permission Set remains unchanged.

For IPsec users, the TOE uses the IPsec/Firewall to control access to the supported network service protocols. The IPsec/Firewall 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/Firewall 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 - The TOE protects deleted objects by making them unavailable to TOE users via the TOE's interfaces. 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 - The TOE allows an administrator to restrict the forwarding of data received from an External Interface to the Shared-medium Interface. The TOE does not provide a pathway or support for commands necessary to achieve network access.
- TSF self-testing - The TOE contains a suite of self tests to test specific security functionality of the TOE. It contains an on-demand Data Integrity Test to verify the integrity of specific TSF Data of the TOE, and an on-demand Code Integrity Test to verify the integrity of TOE executable code files stored on the storage drive.
- Reliable timestamps - The TOE contains a system clock that is used to generate reliable timestamps. In the evaluated configuration, the TOE must be configured to synchronize its system clock with a Network Time Protocol (NTP) server.

3.6 TOE access protection

- Inactivity Timeout - The Control Panel supports an Inactivity Timeout in case users forget to sign out of the Control Panel after signing in.

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 and document storage and retrieval 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, Kerberos, LDAP, NTP, SMTP, syslog, SMB, 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 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.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 Web Services (HTTP), and at the Control Panel.

P.USERNAME.CHARACTER_SET

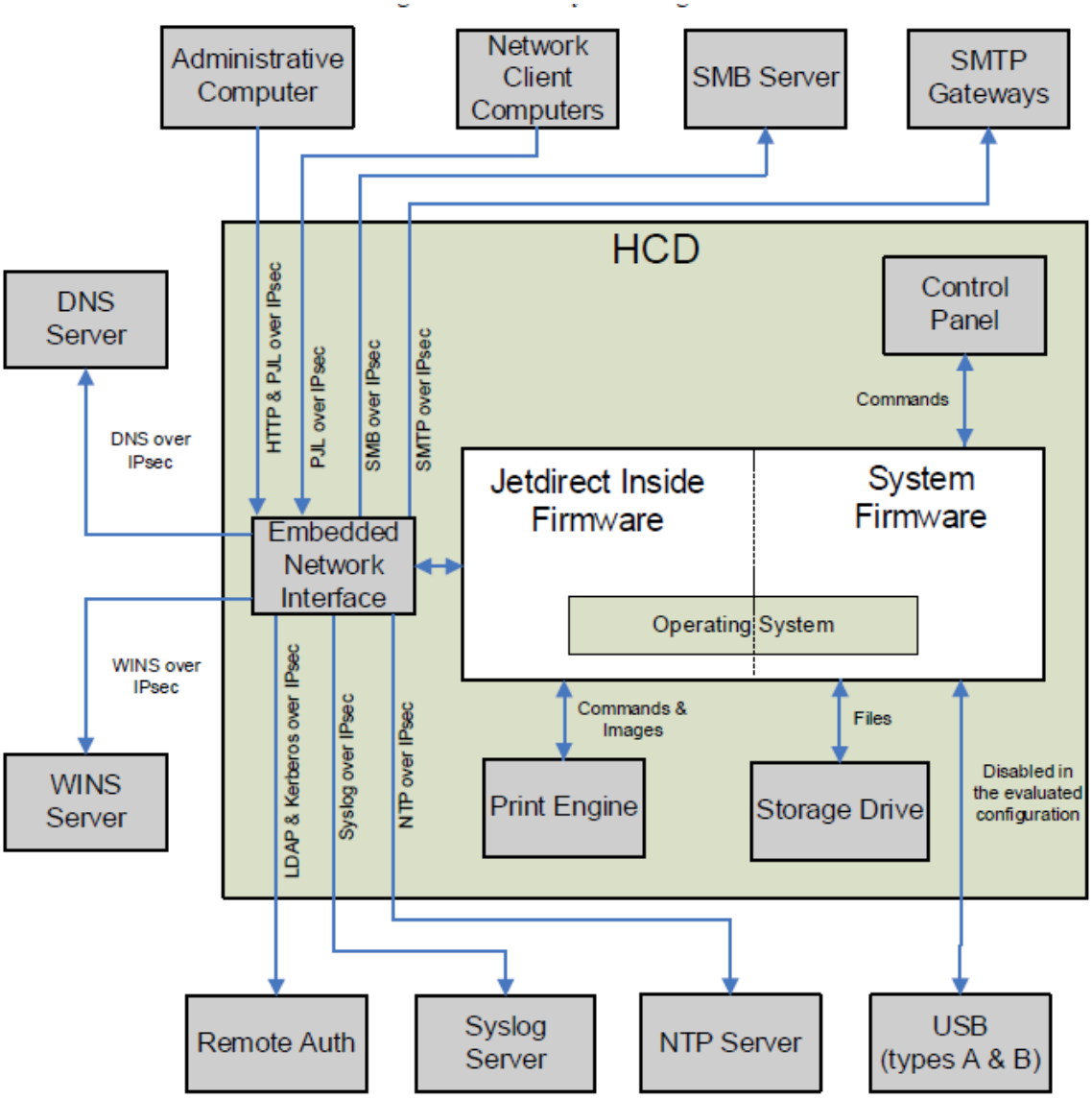
To prevent ambiguous user names in the TOE's audit trail, the user names of the LDAP and Windows Sign In users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

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 can be connected to a wired local network through the embedded Jetdirect Inside print server's built-in Ethernet or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration).



6 Documentation

[CCECG]	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers: HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330, HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725, HP PageWide Enterprise Color MFP 586
[M578_IG]	HP Color LaserJet Enterprise MFP M578 Installation Guide
[M578_UG]	HP Color LaserJet Enterprise MFP M578 User Guide
[M586_IG]	HP PageWide Enterprise Color MFP 586 Installation Guide
[M586_UG]	HP PageWide Enterprise Color MFP 586 User Guide
[M725_IG]	HP Laserjet Enterprise MFP 725 Installation Guide
[M725_UG]	HP Laserjet Enterprise 700 MFP User Guide
[M830_IG]	HP Laserjet Enterprise Flow MFP M830 Installation Guide
[M830_UG]	HP Laserjet Enterprise Flow MFP M830 User Guide
[M880_IG]	HP Color Laserjet Enterprise Flow MFP M880 Installation Guide
[M880_UG]	HP Color Laserjet Enterprise Flow MFP M880 User Guide

7 IT Product Testing

7.1 Developer Testing

Testing was performed by the developer at the HP site in Boise, Idaho, USA. The evaluator notes that the testing is performed both automatically and manually. All tests were passed successfully. The approach for testing was to provide at least one test case for each Security Functional Requirement mapped to the TOE security functionality. The developer reported that all tests were completed successfully.

7.2 Evaluator Testing

The evaluator re-executed a number of developer tests: all 75 automated tests, 3 regular manual tests and 4 manual IPsec tests. The sample was chosen to cover all TSFIs and subsystems classified as SFR-enforcing and supporting. 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. The evaluator examined all potential 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 items 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 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 Inside management via telnet and FTP must be disabled.
• 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/Firewall:
  - 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 JetAdvantage Link 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.

• PC Fax Send 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 (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional specification	ADV_FSP.3	PASS
TOE 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
CM capabilities	ALC_CMC.3	PASS
CM scope	ALC_CMS.3	PASS
Delivery	ALC_DEL.1	PASS
Development security	ALC_DSV.1	PASS
Flaw remediation	ALC_FLR.2	PASS
Life-cycle definition	ALC_LCD.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	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS

Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

The additional recommendation is applicable for

• HP CJA 2600PP (CSEC2020021) – TOE: HP FutureSmart 4.11.0.1 Firmware for the HP LaserJet Enterprise MFP M578,

HP Color LaserJet Managed MFP E78323/E78325/E78330,

HP Color LaserJet Managed MFP E78223/E78228,

HP Color LaserJet Enterprise Flow MFP M880,

HP LaserJet Enterprise Flow MFP M830,

HP LaserJet Enterprise MFP M725, and

HP PageWide Enterprise Color MFP 586 multifunction printers

The evaluators identified a residual vulnerability in the TOEs mentioned above. The vendor HP Inc. has released a fix in an updated firmware version, see https://support.hp.com/usen/document/ish_5000383-5000409-16, which mitigates the vulnerability.

The evaluation was performed using the Evaluation Assurance Level (EAL) 3, augmented by ALC_FLR.2. This means that the evaluators also evaluated the flaw remediation process to verify that the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Additionally, it also includes whether the developer's procedures provide for the corrections of security flaws, for the receipt of flaw reports from TOE users, and for assurance that the corrections introduce no new security flaws.

The evaluator notes that the security patch was not included in the evaluation. It is therefore the responsibility of the individual organization to determine their potential risks and benefits associated with installing newer product versions or additional firmware/software/hardware that was not subject to this evaluation, and by doing so to deviate from the evaluated configuration that has been certified. However, the TOE users are recommended to update their printer firmware to prevent potential exploitation of this vulnerability.

11 Certifier Comments

The certifier is aware of the occurrence of a residual vulnerability in the TOE. The certification is conducted at EAL3 augmented with ALC_FLR.2 indicating that the developer's intention is to maintain and update the TOE in order to keep it relevant over time. The certifier notes that the vendor HP Inc. has released a fix in an updated firmware version, see https://support.hp.com/usen/document/ish_5000383-5000409-16, which mitigates the residual vulnerability.

As the threat landscape is shifting at a high pace, the current security level of printers can swiftly change, as new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. The certifier notes that while updating the application or its environment will put it outside of the evaluated configuration, for many scenarios a reasonable policy would be to keep products up to date with the latest version of the firmware/software. However, the benefit of installing firmware/software updates must be balanced with the potential risks that such changes might have unexpected effect on the behavior of the evaluated security functionality.

12 Glossary

AH	Authentication Header (IPsec)
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
DNS	Domain Name System
EWS	Embedded Web Server
HCD	Hardcopy Device
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
IPsec	Internet Protocol Security
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
OXP	Open Extensibility Platform
OXPd	OXP device layer
PIN	Personal Identification Number
PJL	Printer Job Language
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
USB	Universal Serial Bus
XML	Extensible Markup Language

13 Bibliography

13.1 General

ST	HP HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725, HP PageWide Enterprise Color MFP 586 Security Target, HP Inc., 2021-08-13, 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
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
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0
EP-188	EP-188 Scheme Crypto Policy, CSEC, 2021-10-26 document version 12.0

13.2 Documentation

[CCECG]	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers: HP LaserJet Enterprise MFP M578, HP Color LaserJet Managed MFP E78323/E78325/E78330, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330, HP Color LaserJet Managed MFP E78223/E78228, HP Color LaserJet Enterprise Flow MFP M880, HP LaserJet Enterprise Flow MFP M830, HP LaserJet Enterprise MFP M725, HP PageWide Enterprise Color MFP 586

Installation Guide, HP Inc., 2021-04-07, Edition 1, 9/2021

[M578_IG] HP Color LaserJet Enterprise MFP M578 Installation Guide, HP Inc., 05-2020, Edition 1

[M578_UG] HP Color LaserJet Enterprise MFP M578 User Guide, HP Inc., 05-2020, Edition 1

[M586_IG] HP PageWide Enterprise Color MFP 586 Installation Guide, HP Inc., 05-2020, Edition 1

[M586_UG] HP PageWide Enterprise Color MFP 586 User Guide, HP Inc., 05-2020, Edition 1

[M725_IG] HP Laserjet Enterprise MFP 725 Installation Guide, HP Inc., 05-2020, Edition 1

[M725_UG] HP Laserjet Enterprise 700 MFP User Guide, HP Inc., 05-2020, Edition 1

[M830_IG] HP Laserjet Enterprise Flow MFP M830 Installation Guide, HP Inc., 05-2020, Edition 1

[M830_UG] HP Laserjet Enterprise Flow MFP M830 User Guide, HP Inc., 05-2020, Edition 1

[M880_IG] HP Color Laserjet Enterprise Flow MFP M880 Installation , HP Inc., 05-2020, Edition 1Guide

[M880_UG] HP Color Laserjet Enterprise Flow MFP M880 User Guide, HP Inc., 05-2020, Edition 1

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
2.1	2022-01-18	None.
2.0	2021-11-24	None.
1.25	2021-06-17	None.
1.24.1	2020-12-03	None.
1.24	2020-11-19	None.
1.23.2	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Clarify demonstration of test coverage at EAL2.
SN-18	3.0	Highlighted requirements on the Security Target	Clarifications on the content of the ST.
SN-22	3.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-28	1.0	Updated Procedures for application, evaluation, and certification	Evaluator reports should be received in two batches.
SN-31	1.0	New procedures for site visit oversight and testing oversight	Virtual site visit and testing oversight procedures