
**Swedish Certification Body for IT Security**

# Certification Report - HP CG HCDPP

**Issue: 1.0, 2021-Jul-09**

*Authorisation: Helén Svensson, Lead Certifier , CSEC*

Table of Contents

# 1 Executive Summary

The TOE is the

HP Color LaserJet Enterprise MFP M578,

HP LaserJet Managed Flow MFP E72525/E72530/E72535,

HP Color LaserJet Managed Flow MFP E77822/E77825/E77830,

HP LaserJet Managed Flow MFP E82540/E82550/E82560,

HP Color LaserJet Managed Flow MFP E87640/E87650/E87660, and

HP Color LaserJet Managed Flow MFP E78323/E78325/E78330 with HP FutureSmart 4.11.0.1 Firmware.

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

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

The following firmware modules are included in the TOE.

- System firmware
- Jetdirect Inside firmware

The Security Target claims conformance to:

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

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was completed on 2021-06-30. 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 both confirm both to the evaluation activities in the HCDPP and the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 1 augmented by e.g. ALC_SPD.1.

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

| |
|---|
| 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.<br>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 | CSEC2020014 |
| Name and version of the certified IT product | • HP Color LaserJet Enterprise MFP M578, Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060474<br>• HP LaserJet Managed Flow MFP E72525/E72530/E72535, Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060470<br>• HP Color LaserJet Managed Flow MFP E77822/E77825/E77830, Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060469<br>• HP LaserJet Managed Flow MFP E82540/E82550/E82560, Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060465<br>• HP Color LaserJet Managed Flow MFP E87640/E87650/E87660, Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060464<br>• HP Color LaserJet Managed Flow MFP E78323/E78325/E78330 Jetdirect Inside firmware version: JSI24110014 System firmware version: 2411097_060469 |
| Security Target Identification | HP Color LaserJet Enterprise MFP M578, HP LaserJet Managed Flow MFP E72525/E72530/E72535, HP Color LaserJet Managed Flow MFP E77822/E77825/E77830, HP LaserJet Managed Flow MFP E82540/E82550/E82560, HP Color LaserJet Managed Flow MFP E87640/E87650/E87660, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330, Security Target, HP Inc., 2021-04-13, document version 1.1 |
| EAL | for CCRA and EA_MLA:<br>Protection Profile for Hardcopy Devices v1.0 with Errata #1, including ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, and AVA_VAN.1<br><br>for SOGIS:<br>EAL 1 + ASE_SPD.1 |

| | |
|---|---|
| Sponsor | HP Inc. |
| Developer | HP Inc. |
| ITSEF | atsec information security AB |
| Common Criteria version | 3.1 release 5 |
| CEM version | 3.1 release 5 |
| QMS version | 1.25 |
| Scheme Notes Release | 18.0 |
| Recognition Scope | CCRA, SOGIS, EA/MLA |
| Certification date | 2021-07-09 |

# 3 Security Policy

The TOE provides the following security services:

- Identification, authentication, and authorization to use HCD functions
- Access control
- Data encryption (a.k.a. cryptography)
- Trusted communications
- Administrative roles
- Auditing
- Trusted operation
- PSTN Fax-network Separation

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

## 3.1 Identification, Authentication, and Authorization to Use HCD Functions

The following table shows the Internal and External Authentication mechanisms supported by the TOE in the evaluated configuration and maps the mechanisms to the interfaces that use them. The PJL interface does not appear in this table because the PJL interface does not perform authentication of users.

| Authentication type | Mechanism name | Supported interfaces |
|---|---|---|
| Internal Authentication | Local Device Sign In | Control Panel, EWS, REST |
| External Authentication | LDAP Sign In | Control Panel, EWS |
| | Windows Sign In | Control Panel, EWS, REST |

## 3.2 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 PSs used to define roles also affect the access control of each user. The access control mechanism for User Data is explained in more detail in the TSS for FDP_ACF.1.

Depending on the TOE model, the TOE contains either one or two field-replaceable, nonvolatile storage devices. These storage devices are disk-based SEDs whose cryptographic functions have been FIPS 140-2 validated. Together with the drive-lock password, the SEDs ensures that TSF Data and User Data on the drives is not stored as plaintext on the storage device.

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

## 3.3 Data Encryption (a.k.a. cryptography)

### 3.3.1 IPsec

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

### 3.3.2 Drive-lock Password

For secure storage, all TOE models contain one to two field-replaceable, nonvolatile storage devices. These storage devices are disk-based, self-encrypting drives (SEDs) that are FIPS 140-2 validated.

The SEDs in the TOE use the same 256-bit "drive-lock password" as the border encryption value (BEV), which is used to unlock the data on the drives. The BEV is generated by the TOE using a CTR_DRBG(AES-256) algorithm and is stored as a key chain of one in non-field replaceable nonvolatile storage (i.e., EEPROM, and if two SEDs, also embedded MultiMediaCard (eMMC)) located inside the TOE. The CTR_DRBG(AES-256) uses the Advanced Encryption Standard-Counter (AES-CTR) algorithm.

### 3.3.3 Digital Signatures for Trusted Update

The TOE uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to verify the authenticity of the signed update images. The TOE's EWS interface allows an administrator to verify and install the signed update images.

### 3.3.4 Digital Signatures for TSF Testing

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

### 3.3.5 Cryptographic Implementations/Modules

The TOE uses multiple cryptographic implementations to accomplish its cryptographic functions. Table 4 provides the complete list of cryptographic implementations used to satisfy the [HCDPP] cryptographic requirements and maps the cryptographic implementations to the firmware modules.

| Firmware module | Cryptographic implementation | Usage |
|---|---|---|
| Jetdirect Inside firmware | HP FutureSmart OpenSSL FIPS Object Module 2.0.4 | Drive-lock password (BEV) generation |
| | HP FutureSmart QuickSec 5.1 | IPsec |

| | | |
|---|---|---|
| System firmware | HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 | TSF testing |
| | HP FutureSmart Rebex Total Pack 2017 R1 2470159 | Trusted update |

## 3.4 Trusted Communications

The TOE uses IPsec to protect the communications between the TOE and trusted IT entities as well as between the TOE and client computers. IPsec provides assured identification of the endpoints. It implements IKEv1 and transport mode. The TOE also supports both X.509v3 certificates and pre-shared keys (PSKs) for endpoint authentication.

## 3.5 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.

## 3.6 Auditing

The TOE supports both internal and external storage of audit records. The evaluated configuration requires the use of an external syslog server for external audit record storage. The connection between the TOE and the syslog server is protected using IPsec. No unauthorized access to the audit records is allowed by the TOE.

## 3.7 Trusted Operation

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

The TOE contains TSF testing functionality referred to as Whitelisting to help ensure only authentic, known-good firmware files that have not been tampered with are loaded into memory. Whitelisting uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to validate the firmware files.

## 3.8 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.

# 4 Assumptions and Clarification of Scope

## 4.1 Assumptions

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

A.PHYSICAL - Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.

A.TRUSTED_ADMIN - TOE Administrators are trusted to administer the TOE according to site security policies.

A.TRAINED_USERS - Authorized Users are trained to use the TOE according to site security policies.

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

## 4.2 Clarification of Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 5 Architectural Information

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

The TOE's operating system is the Windows Embedded CE 6.0 R3 running on an Arm Cortex-A8 processor.

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

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

The Web Services (WS) interfaces allow administrators to externally manage the TOE. The evaluated configuration only supports the REST Web Services interface. The REST Web Services interface is protected using IPsec.

For design reasons, only one computer can be used as the Administrative Computer for the TOE in the evaluated configuration. This computer is used for administration of the TOE. All other client computers connecting to the TOE to perform non-administrative tasks are known as Network Client Computers.

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

The PJL interface is used by unauthenticated users via Network Client Computers to submit print jobs and receive job status (e.g., view the print queue). The unauthenticated users use PJL over an IPsec connection. It is also used in a non-administrative capacity by the Administrative Computer to send print jobs to the TOE as well as to receive job status. In general, PJL supports password-protected administrative commands, but in the evaluated configuration these commands are disabled.

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

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

The TOE supports the auditing of security-relevant functions by generating and forwarding audit records to an external syslog server. It supports both internal and external storage of audit records. The TOE uses IPsec to protect the communications between itself and the syslog server.

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

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

Both administrative and non-administrative users can access the Control Panel.

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

All TOE models contain at least one field-replaceable nonvolatile storage disk drive. This drive must be FIPS 140-2 validated SED. Depending on the TOE model, this drive may come pre-installed or the TOE may require the installation of the HP TAA Version Secure Hard Disk Drive accessory prior to deploying the TOE.

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

# 6 Documentation

- HP Color LaserJet Enterprise MFP M578 User Guide [M578-UG]
- Common Criteria Evaluated Configuration Guide for HP Multifunction Printers, HP Color LaserJet Enterprise MFP M578, HP LaserJet Managed Flow MFP E72525/E72530/E72535, HP Color LaserJet Managed Flow MFP E77822/E77825/E77830, HP LaserJet Managed Flow MFP E82540/E82550/E82560, HP Color LaserJet Managed Flow MFP E87640/E87650/E87660, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330 [CCECG]
- HP Color LaserJet Enterprise MFP M578 M578dn, M578f, M578c, M578z Installation Guide [M578-IG]
- HP LaserJet Managed MFP E72525, E72530, E72535 HP LaserJet Managed Flow MFP E72525, E72530, E72535 HP Color LaserJet Managed MFP E78323, E78325, E78330 HP Color LaserJet Managed Flow MFP E78323, E78325, E78330 User Guide [E725_E783_UG]
- HP LaserJet MFP E72500 Engine Install Guide [E725-IG]
- HP Color LaserJet Managed MFP E78323, E78325, E78330 HP Color LaserJet Managed MFP E77822, E77825, E77830 Engine Installation Guide [E783_E778-IG]
- HP LaserJet Managed MFP E72525, E72530, E72535 HP LaserJet Managed Flow MFP E72525, E72530, E72535 HP Color LaserJet Managed MFP E77822, E77825, E77830 HP Color LaserJet Managed Flow MFP E77822, E77825, E77830 User Guide [E778-UG]
- HP LaserJet Managed MFP E82540, E82550, E82560 HP LaserJet Managed Flow MFP E82540, E82550, E82560 HP Color LaserJet Managed MFP E87640, E87650, E87660 HP Color LaserJet Managed Flow MFP E87640, E87650, E87660 User Guide [E825_E876-UG]
- HP LaserJet Managed Flow MFP E82540-E82560 Engine Install Guide [E825-IG]
- HP Color LaserJet Managed Flow MFP E87640-E87660 Engine Install Guide [E876-IG]

# 7 IT Product Testing

## 7.1 Developer Testing

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

## 7.2 Evaluator Testing

The evaluator performed testing remotely by connecting to the test environment using Microsoft Remote Desktop (RDP). The developers setup the test environment with the actual TOE models in Boise, Idaho, USA. The testing was performed between 2020-08-14 and 2021-01-22. The tests included both automated and manual tests which the evaluator executed successfully.

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

| TOE Name (hardware models) | System Firmware Version | Jetdirect Inside Firmware Version |
|---|---|---|
| HP Color LaserJet Enterprise MFP M578 | 2411097_060474 | JSI24110014 |
| HP Color LaserJet Managed Flow MFP E78323 | 2411097_060469 | JSI24110014 |
| HP Color LaserJet Managed Flow MFP E87650 | 2411097_060464 | JSI24110014 |

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

All the actual test results were consistent to the expected test results.

## 7.3 Penetration Testing

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

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

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

The following models were tested:

| TOE Name (hardware models) | System Firmware Version | Jetdirect Inside Firmware Version |
|---|---|---|
| HP Color LaserJet Enterprise MFP M578 | 2411097_060474 | JSI24110014 |
| HP Color LaserJet Managed Flow MFP E78323 | 2411097_060469 | JSI24110014 |
| HP Color LaserJet Managed Flow MFP E87650 | 2411097_060464 | JSI24110014 |

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

The evaluator examined the results from the penetration test and provided a summarization within the "Evaluator penetration testing CG HCD PP". The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec which was the expected outcome.

# 8 Evaluated Configuration

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

- 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.
- 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.
- Only X.509v3 certificates and pre-shared key are supported methods for IPsec authentication (IPsec authentication using Kerberos is not supported).
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Mandatory Sign-in must be enabled (this disables the Guest role).
- SNMP must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to 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.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the 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.
- Remote Configuration Password must not be set.
- OAUTH2 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.
- Firmware updates through REST Web Services is disallowed.

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

- A Domain Name System (DNS) server
- A Network Time Service (NTS) server
- One administrative client computer connected to the TOE in the role of an Administrative Computer. It must contain a web browser
- One or both of the following:
  - Lightweight Directory Access Protocol (LDAP) server
  - Windows domain controller/Kerberos server
- A syslog server
- A Windows Internet Name Service (WINS) server

The following components are optional in the Operational Environment:

- Client computers connected to the TOE in a non-administrative computer role
- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- Microsoft SharePoint
- The following remote file systems:
  - File Transfer Protocol (FTP)
  - Server Message Block (SMB)
- A Simple Mail Transfer Protocol (SMTP) gateway
- Telephone line connection

# 9 Results of the Evaluation

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

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

The evaluators' overall verdict is PASS.

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

Note that the evaluators have used a notation similar to assurance classes for PP assurance activities that does not belong to a particular assurance class in CC.

For PP requirements that are related to existing assurance classes, the evaluators have used a notation similar to assurance components for the requirements.

# 10 Evaluator Comments and Recommendations

None.

# 11 Glossary

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AH | Authentication Header (IPsec) |
| Arm | Advanced RISC Machine |
| BEV | Border Encryption Value |
| CC | Common Criteria |
| cPP | Collaborative Protection Profile |
| CSEC | The Swedish Certification Body for IT Security |
| CTR | Counter mode |
| CTR_DRBG | Counter mode DRBG |
| DNS | Domain Name System |
| DRBG | Deterministic Random Bit Generator |
| DSS | Digital Sending Software |
| EAL | Evaluated Assurance Level |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| ESP | Encapsulating Security Payload (IPsec) |
| EWS | Embedded Web Server |
| FIPS | Federal Information Processing Standard |
| HCD | Hardcopy Device |
| HCDPP | Hardcopy Device Protection Profile |
| HP | Hewlett-Packard |
| I&A | Identification and Authentication |
| IKE | Internet Key Exchange (IPsec) |
| IP | Internet Protocol |
| IPv4 | IP version 4 |
| IPv6 | IP version 6 |
| IPsec | Internet Protocol Security |
| ISAKMP | Internet Security Association Key Management Protocol (IPsec) |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MFP | Multifunction Printer |
| NIAP | National Information Assurance Partnership |
| NTLM | Microsoft NT LAN Manager |
| NTS | Network Time Service |
| OSP | Organizational Security Policy |
| OXP | Open Extensibility Platform |
| OXPd | OXP device layer |
| PJL | Printer Job Language |
| PKCS | Public-Key Cryptography Standards |
| PP | Protection Profile |
| PSK | Pre-Shared Key |
| PSTN | Public Switched Telephone Network |
| REST | Representational State Transfer |
| RSA | Rivest-Shamir-Adleman |
| SED | Self-Encrypting Drive |
| SFP | Single-Function Printer |
| SHA | Secure Hash Algorithm |
| SHS | Secure Hash Standard |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SP | Special Publication |
| SPD | Security Problem Definition (CC) |

| | |
|---|---|
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSS | TOE Summary Specification |
| UI | User Interface |
| USB | Universal Serial Bus |
| WINS | Windows Internet Name Service |
| WLAN | Wireless Local Area Network |
| WS | Web Services |

# 12 Bibliography


| | |
|---|---|
| ST | HP Color LaserJet Enterprise M554/M555, HP Color LaserJet Enterprise M652/M653, HP Color LaserJet Managed E65050/E65060 Security Target, 2021-04-13, Version 1.1 |
| HCDPPv1.0 | Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP, 2015-09-10, Version 1.0 |
| ERRATA | Protection Profile for Hardcopy Devices - v1.0, Errata #1, June 2017 |
| CCECG | Common Criteria Evaluated Configuration Guide for HP Multifunction Printers, HP Color LaserJet Enterprise MFP M578, HP LaserJet Managed Flow MFP E72525/E72530/E72535, HP Color LaserJet Managed Flow MFP E77822/E77825/E77830, HP LaserJet Managed Flow MFP E82540/E82550/E82560, HP Color LaserJet Managed Flow MFP E87640/E87650/E87660, HP Color LaserJet Managed Flow MFP E78323/E78325/E78330, Edition 1, 5/2021 |
| M578-UG | HP Color LaserJet Enterprise MFP M578 User Guide, Edition 1, 10/2020 |
| M578-IG | HP Color LaserJet Enterprise MFP M578 M578dn, M578f, M578c, M578z Installation Guide, 2020 |
| E725_E783_UG | HP LaserJet Managed MFP E72525, E72530, E72535<br>HP LaserJet Managed Flow MFP E72525, E72530, E72535<br>HP Color LaserJet Managed MFP E78323, E78325, E78330<br>HP Color LaserJet Managed Flow MFP E78323, E78325, E78330 User Guide, Edition 2, 7/2020 |
| E725-IG | HP LaserJet MFP E72500 Engine Install Guide, 2019 |
| E783_E778-IG | HP Color LaserJet Managed MFP E78323, E78325, E78330<br>HP Color LaserJet Managed MFP E77822, E77825, E77830<br>Engine Installation Guide, 2020 |
| E778-UG | HP LaserJet Managed MFP E72525, E72530, E72535<br>HP LaserJet Managed Flow MFP E72525, E72530, E72535<br>HP Color LaserJet Managed MFP E77822, E77825, E77830<br>HP Color LaserJet Managed Flow MFP E77822, E77825, E77830 User Guide, Edition 3, 2/2019 |
| E825_E876-UG | HP LaserJet Managed MFP E82540, E82550, E82560<br>HP LaserJet Managed Flow MFP E82540, E82550, E82560<br>HP Color LaserJet Managed MFP E87640, E87650, E87660<br>HP Color LaserJet Managed Flow MFP E87640, E87650, E87660 User Guide, Edition 3, 2/2019 |
| E825-IG | HP LaserJet Managed Flow MFP E82540-E82560 Engine Install Guide, 2019 |
| E876-IG | HP Color LaserJet Managed Flow MFP E87640-E87660 Engine Install Guide, 2019 |
| CEM | Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004 |
| SP-002 | SP-002 Evaluation and Certification, CSEC, 2021-06-04, document version 33.0 |
| SP-188 | SP-188 Scheme Crypto Policy, CSEC, 2021-06-07, document version 11.0 |

# Appendix A Scheme Versions

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

## A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.24.1 valid from 2020-12-03

QMS 1.25 valid from 2021-06-17

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.25". The certifier concluded that, from QMS 1.24.1 to the current QMS 1.25, there are no changes with impact on the result of the certification.

## A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 21 - NIAP PP Certifications
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs
- Scheme Note 25 - Use of CAVP-tests in CC evaluations