*Agenzia per la Cybersicurezza Nazionale*

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ve.3.1 rel. 5

| | |
|---|---|
| **Certificato n.** *(Certificate No.)* | 09/2024 |
| **Rapporto di Certificazione** *(Certification Report)* | OCSI/CERT/ATS/02/2024/RC, v 1.0. |
| **Decorrenza** *(Date of 1st Issue)* | 18 dicembre 2024 |
| **Nome e Versione del Prodotto** *(Product Name and Version)* | HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware |
| **Sviluppatore** *(Developer)* | HP Inc. |
| **Tipo di Prodotto** *(Type of Product)* | Dispositivi multifunzione |
| **Conformità a PP** *(PP Conformance)* | Protection Profile for Hardcopy Devices v1.0 with Errata#1 |
| **Funzionalità di sicurezza** *(Conformance of Functionality)* | Funzionalità conformi a PP, CC Parte 2 estesa |

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
*(CCRA recognition for components up to EAL2 and ALC_FLR only)*

Riconoscimento SOGIS MRA per componenti fino a EAL4
*(SOGIS MRA recognition for components up to EAL4)*

Roma, 18 dicembre 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

*[ORIGINAL SIGNED]*

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

*The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5* for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Organismo di Certificazione della Sicurezza Informatica

*Agenzia per la Cybersicurezza Nazionale*

*Servizio Certificazione e Vigilanza*

Organismo di Certificazione della Sicurezza Informatica

# Certification Report

## HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware

OCSI/CERT/ATS/02/2024/RC

Version 1.0

18 December 2024

# Courtesy translation

**Disclaimer**: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

# 1 Document revisions

| Version | Author | Information | Date |
|---|---|---|---|
| 1.0 | OCSI | First issue | 18/12/2024 |

# 2 Table of contents

1 Document revisions ..... 3
2 Table of contents ..... 4
3 Acronyms ..... 6
3.1 National scheme ..... 6
3.2 CC and CEM ..... 6
3.3 Other acronyms ..... 6
4 References ..... 9
4.1 Normative references and national Scheme documents ..... 9
4.2 Technical documents ..... 9
5 Recognition of the certificate ..... 11
5.1 European recognition of CC certificates (SOGIS-MRA) ..... 11
5.2 International recognition of CC certificates (CCRA) ..... 11
6 Statement of Certification ..... 12
7 Summary of the evaluation ..... 13
7.1 Introduction ..... 13
7.2 Executive summary ..... 13
7.3 Evaluated product ..... 14
7.3.1 TOE architecture ..... 15
7.3.2 TOE security features ..... 16
7.4 Documentation ..... 19
7.5 Protection Profile conformance claims ..... 19
7.6 Functional and assurance requirements ..... 19
7.7 Evaluation conduct ..... 19
7.8 General considerations about the certification validity ..... 20
8 Evaluation outcome ..... 21
8.1 Evaluation results ..... 21
8.2 Additional assurance activities ..... 22
8.3 Recommendations ..... 22
9 Annex A – Guidelines for the secure usage of the product ..... 23
9.1 TOE delivery ..... 23
9.2 Identification of the TOE by the User ..... 25
9.3 Installation, configuration, and secure usage of the TOE ..... 25
10 Annex B – Evaluated configuration ..... 26

10.1 TOE operational environment ..... 27
11 Annex C – Test activity ..... 28
11.1 Test configuration ..... 28
11.2 Functional and independent tests performed by the Evaluators ..... 28
11.3 Vulnerability analysis and penetration tests ..... 29

# 3 Acronyms

## 3.1 National scheme

| | |
|---|---|
| **DPCM** | Decreto del Presidente del Consiglio dei ministri |
| **LGP** | Linea Guida Provvisoria |
| **LVS** | Laboratorio per la Valutazione della Sicurezza |
| **NIS** | Nota Informativa dello Schema |
| **OCSI** | Organismo di Certificazione della Sicurezza Informatica |

## 3.2 CC and CEM

| | |
|---|---|
| **CC** | Common Criteria |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CEM** | Common Evaluation Methodology |
| **cPP** | collaborative Protection Profile |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **PP** | Protection Profile |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **SOGIS-MRA** | Senior Officials Group Information Systems Security – Mutual Recognition Agreement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **TSFI** | TSF Interface |

## 3.3 Other acronyms

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **AH** | Authentication Headers |
| **BEV** | Border Encryption Value |
| **BLE** | Bluetooth Low Energy |
| **CBC** | Cipher Block Chaining |
| **CTR_DRBG** | Counter (CTR) mode block cipher algorithm DRBG |
| **DH** | Diffie-Hellman |
| **DNS** | Domain Name System |
| **DRBG** | Deterministic Random Bit Generator |

| | |
|---|---|
| **DSA** | Digital Signature Algorithm |
| **ECB** | Electronic Code Book |
| **EWS** | Exchange Web Services |
| **FFC** | Finite Field Cryptography |
| **FIPS** | Federal Information Processing Standards |
| **FTP** | File Transfer Protocol |
| **HCD** | Hardcopy Device |
| **HTTP** | HyperText Transfer Protocol |
| **HTTPS** | Hyper Text Transfer Protocol Secure |
| **IKE** | Internet Key Exchange |
| **IPsec** | Internet Protocol Security |
| **IPv4** | Internet Protocol version 4 |
| **IPv6** | Internet Protocol version 6 |
| **ISAKMP** | Internet Security Association and Key Management Protocol |
| **IT** | Information Technology |
| **KAS** | Key Agreement Scheme |
| **LAN** | Local Area Network |
| **LCD** | Liquid Crystal Display |
| **LDAP** | Lightweight Directory Access Protocol |
| **MFP** | Multi-Function Printer |
| **NFC** | Near Field Communication |
| **NTLM** | New Technology LAN Manager |
| **OXPd** | Open Extensibility Platform device |
| **PIN** | Personal Identification Number |
| **PJL** | Printer Job Language |
| **PKCS** | Public-Key Cryptography Standards |
| **PSK** | Pre-shared Key |
| **RDP** | Remote Desktop Protocol |
| **REST** | Representational State Transfer |
| **RSA** | Rivest, Shamir, Adleman |
| **SED** | Self-encrypting Drive |
| **SHA** | Secure Hash Algorithm |
| **SMB** | Server Message Block |
| **SMTP** | Simple Mail Transfer Protocol |
| **SNMP** | Simple Network Management Protocol |

| | |
|---|---|
| **SPI** | Serial Peripheral Interface |
| **SSC** | Security Subsystem Class |
| **TCG** | Trusted Computing Group |
| **TCP** | Transmission Control Protocol |
| **UDP** | User Datagram Protocol |
| **UI** | User Interface |
| **USB** | Universal Serial Bus |
| **VTL** | Virtual Test Laboratory |
| **WINS** | Windows Internet Naming Service |
| **WLAN** | Wireless Local Area Network |
| **WS** | Web Services |
| **XML** | eXtensible Markup Language |

# 4 References

## 4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 – Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

## 4.2 Technical documents

[CCECG] Common Criteria Evaluated Configuration Guide for HP Single-function Printers HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP

LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, HP Color LaserJet Managed E75245, HP Inc, Edition 1, 2 July 2024

[ETR] Final Evaluation Technical Report HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware, version 2.0, 11 October 2024

[HCDPP] Protection Profile for Hardcopy Devices, IPA, NIAP, and the MFP Technical community, version 1.0, 10 September 2015

[HCDPP-ER] Protection Profile for Hardcopy Devices – version 1.0 Errata #1, June 2017

[ST] HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612 HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, HP Color LaserJet Managed E75245, version 1.0, 25 October 2024

# 5 Recognition of the certificate

## 5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all declared assurance components up to EAL4.

## 5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components up to EAL2 and ALC_FLR only.

# 6 Statement of Certification

The Target of Evaluation (TOE) is "**HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware**", developed by HP, Inc.

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

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 for the assurance components included in the PP [HCDPP], according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

# 7 Summary of the evaluation

## 7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the TOE "HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

## 7.2 Executive summary

| | |
|---|---|
| **TOE name** | HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware |
| **Security Target** | HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612 HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, HP Color LaserJet Managed E75245, Version 1.0, 25 October 2024 [ST] |
| **Evaluation Assurance Level** | Conformant to PP including the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 |
| **Developer** | HP, Inc. |
| **Sponsor** | HP, Inc. |
| **LVS** | atsec information security s.r.l. |
| **CC version** | 3.1 Rev. 5 |
| **PP conformance claim** | Protection Profile for Hardcopy Devices v1.0 [HCDPP] with Errata#1 [HCDPP-ER] |
| **Evaluation starting date** | 20 March 2024 |
| **Evaluation ending date** | 14 October 2024 |

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

## 7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The Target of Evaluation (TOE) is identified as follows HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware.

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.

All TOE models use the same Jetdirect Inside firmware version:

- JSI25077205.

The Table 1 shows the HCD models included in the evaluation and the System firmware version.

| **Model name** | **Product number** | **System firmware version** |
|---|---|---|
| HP Color Laserjet Enterprise M751n | T3U43A | 2507252_045129 |
| HP Color Laserjet Enterprise M75dn | T3U44A | 2507252_045129 |
| HP Color LaserJet Managed E75245dn | T3U46A | 2507252_045129 |
| HP LaserJet Enterprise M610dn | 7PS82A | 2507252_046110 |
| HP LaserJet Enterprise M611dn | 7PS84A | 2507252_046110 |
| HP LaserJet Enterprise M611x | 7PS85A | 2507252_046110 |
| HP LaserJet Enterprise M612dn | 7PS86A | 2507252_046110 |
| HP LaserJet Enterprise M612x | 7PS87A | 2507252_046110 |
| HP Color LaserJet Enterprise M856dn | T3U51A | 2507252_046112 |
| HP Color LaserJet Enterprise M856x | T3U52A | 2507252_046112 |
| HP LaserJet Enterprise M507dn | 1PV87A | 2507252_046139 |
| HP LaserJet Enterprise M507x | 1PV88A | 2507252_046139 |
| HP LaserJet Enterprise M507dng | 1PV89A | 2507252_046139 |

Table 1 - TOE hardware and firmware reference

All TOE models use the Windows Embedded CE 6.0 R3 operating system running on an Arm Cortex-A8 processor.

For a detailed description of the TOE, consult sections 1.4 and 1.5 of the Security Target [ST]. The most significant aspects are summarized below.

### 7.3.1 TOE architecture

The TOE is designed to be shared by many client computers and human users. It performs the functions of printing and storing of documents. It can be connected to a local network through the embedded Jetdirect Inside'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 except when the administrator performs trusted update via the USB).

The TOE's operating system is Windows Embedded CE 6.0 R3[1] running on an Arm Cortex-A8 processor. The TOE supports Local Area Network (LAN) capabilities. The LAN is used to communicate with the administrative computer and several trusted IT entities. Some TOE models include support for Wireless LAN (WLAN), but the WLAN must be disabled in the evaluated configuration. The TOE 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 Administrative Computer connects to the TOE using IPsec. This computer can administer the TOE using the following interfaces over the IPsec connection.

- Embedded Web Server (EWS).
- Representational state transfer (REST) Web Services.

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

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

For design reasons, only one computer can be used as the Administrative Computer for the TOE in the evaluated configuration. This computer is used for administration of the TOE.

All other client computers connecting to the TOE to perform non-administrative tasks are known as Network Client Computers in the ST. Network Client Computers connect to the TOE to submit print jobs to the TOE using the Printer Job Language (PJL) interface. They can also receive job status from the TOE using PJL. The PJL interface connection is protected using IPsec. The PJL interface is used by unauthenticated users via Network Client Computers to submit print jobs and receive job status (e.g., view the print queue). The unauthenticated users use PJL over an IPsec connection. It is also used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL over IPsec to send print jobs to the TOE as well as to receive job status. In general, PJL supports password-protected administrative commands, but in the evaluated configuration, these commands are disabled. The PJL interface is defined as PJL data sent to port 9100.

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

TOE can send email alert messages to administrator-specified email addresses, mobile devices, or to a website. The TOE supports protected communications between itself and Simple Mail Transfer

[1] HP monitors vulnerabilities in Windows Embedded CE and performs Vulnerability Assessment and Penetration Testing (VAPT) for known and unknown vulnerabilities.

Protocol (SMTP) gateways. It uses IPsec to protect the communication with the SMTP gateway. The TOE can only protect unencrypted email up to the SMTP gateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

The TOE supports a remote file system for storing and retrieving backup files during Back up and Restore operations and uses IPsec to protect the communication to the remote file system.

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 and a physical home screen button 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, Kerberos).

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

### 7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sections 1.5.3 and 7.1 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

#### *7.3.2.1 Auditing*

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

#### *7.3.2.2 Data Encryption (a.k.a. cryptography)*

*IPsec*

The TOE's IPsec supports both PSKs and X.509v3 certificates for authentication, the ESP, ISAKMP, IKEv1 protocol, and the following cryptographic algorithms: DH, DSA, RSA, AES-CBC, AES-ECB, SHA-based HMACs, PKCS#1 v1.5 signature generation and verification, and CTR_DRBG(AES). It supports multiple DH groups, transport mode, and uses Main Mode for Phase 1 exchanges in IKEv1. The IKEv1 uses the dhEphem scheme to implement the KAS FFC algorithm when establishing a protected communication channel. DSA key generation is a prerequisite for KAS FFC when using DH ephemeral. The IKEv1 uses imported RSA-based X.509v3 certificates to authenticate the connections. The RSA authentication is accomplished using the IKEv1 digital signature authentication method.

*Drive-lock Password*

For secure storage, all TOE models contain one field-replaceable, nonvolatile storage device that is a disk-based, self-encrypting drive (SED). The SED in the TOE uses the 256-bit "drive-lock password" as the border encryption value (BEV), which is used to unlock the data on the drive. The BEV is generated by the TOE using a CTR_DRBG(AES-256) algorithm and is stored as a key chain of one in non-field replaceable nonvolatile storage (SPI flash and EEPROM) located inside the TOE.

*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.

*Digital signatures for TSF testing*

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

*Cryptographic implementations/modules*

The TOE uses multiple cryptographic implementations to accomplish its cryptographic functions. Table 2 provides the complete list of cryptographic implementations and maps them to the firmware models.

| 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 |

Table 2 - TOE cryptographic implementations

The field-replaceable SED also contains a cryptographic implementation within the drive called the "Seagate Secure® TCG Opal SSC Self-Encrypting Drive." This implementation is based on the Trusted Computing Group's (TCG) Opal Security Subsystem Class (SSC) specification. This implementation has been separately CC certified by the SED's manufacturer. The cryptographic algorithms in this implementation are not claimed in the [ST].

*7.3.2.3 Identification, Authentication, and Authorization to Use HCD Functions*

The following Table 3 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.

| 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 |

Table 3 - TOE authentication mechanisms and their supported interfaces

#### *7.3.2.4 Access Control*

The TOE enforces access control on TSF data and User Data. Each piece of User Data is assigned ownership and access to the data is limited by the access control mechanism. The PSs used to define roles also affect the access control of each user. The TOE contains one field-replaceable, non-volatile storage device that is a disk-based SED whose cryptographic functions have been CC certified outside of this evaluation. Together with the drive-lock password, the SED ensures that TSF Data and User Data on the drive is not stored as plaintext.

#### *7.3.2.5 Image Overwrite*

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

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

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

#### *7.3.2.6 Trusted Communications*

The TOE uses IPsec to protect the communications between the TOE and trusted IT entities as well as between the TOE and the Administrative Computer. 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.

#### *7.3.2.7 Administrative Roles*

The TOE supports administrative and non-administrative roles. Assignment to these roles is controlled by the TOE's administrator. In the case of a user authenticated using an External Authentication mechanism (Windows Sign In and LDAP Sign In), the roles are implemented as permission sets. In the case of a user authenticated using an Internal Authentication mechanism (Local Device Sign In), only an administrative account exists.

#### *7.3.2.8 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 Trusted operation 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.

## 7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.3 of this report.

## 7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance to the following Protection Profiles:

- Protection Profile for Hardcopy Devices, Version 1.0 [HCDPP].
- Protection Profile for Hardcopy Devices – v1.0 Errata #1 [HCDPP-ER].

## 7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived by extension from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims exact conformance to the Protection Profile for Hardcopy Devices [HCDPP], all the SFRs from such PP are included.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

## 7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM]. Furthermore, all specific

assurance activities required by the Protection Profile for Hardcopy Devices [HCDPP] have been carried out.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security s.r.l.

The evaluation was completed on October 14th, 2024, with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on October 22nd, 2024. Then, the Certification Body issued this Certification Report.

## 7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration". Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

# 8 Evaluation outcome

## 8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the PP [HCDPP], with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 4 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level defined by the SARs included in the PP [HCDPP].

| **Assurance classes and components** | | **Verdict** |
|---|---|---|
| **Security Target evaluation** | **Class ASE** | Pass |
| Conformance claims | ASE_CCL.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| ST introduction | ASE_INT.1 | Pass |
| Security objectives for the operational environment | ASE_OBJ.1 | Pass |
| Stated security requirements | ASE_REQ.1 | Pass |
| Security problem definition | ASE_SPD.1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |
| **Development** | **Class ADV** | Pass |
| Basic functional specification | ADV_FSP.1 | Pass |
| **Guidance documents** | **Class AGD** | Pass |
| Operational user guidance | AGD_OPE.1 | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |
| **Life cycle support** | **Class ALC** | Pass |
| Labelling of the TOE | ALC_CMC.1 | Pass |
| TOE CM coverage | ALC_CMS.1 | Pass |
| **Test** | **Class ATE** | Pass |
| Independent testing - conformance | ATE_IND.1 | Pass |
| **Vulnerability assessment** | **Class AVA** | **Pass** |
| Vulnerability survey | AVA_VAN.1 | Pass |

Table 4 - Final verdicts for assurance requirements

## 8.2 Additional assurance activities

The Protection Profile for Hardcopy Devices [HCDPP] includes additional assurance activities specific to the TOE technology type, and are required for exact conformance to the PP.

The Evaluators used for the PP assurance activities a notation similar to assurance components of existing CC assurance classes. The objective of these sub-activities is to determine whether the requirements of the assurance activities included in the PP are met.

Table 5 summarizes the final verdict of the PP assurance activities carried out by the LVS.

| **PP assurance activities**[2] | | **Verdict** |
|---|---|---|
| **ASE: Security Target evaluation** | ASE_HCDPP.1 | Pass |
| **AGD: Guidance documents** | AGD_HCDPP.1 | Pass |
| **ALC: Life cycle support** | ALC_HCDPP.1 | Pass |
| **ATE: Tests** | ATE_HCDPP.1 | Pass |
| **AVA: Vulnerability assessment** | AVA_HCDPP.1 | Pass |
| **AEN: Entropy Description** | AEN_HCDPP.1 | Pass |
| **AKM: Key Management Description** | AKM_HCDPP.1 | Pass |

Table 5 - Final verdicts for PP [HCDPP] assurance activities

## 8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the TOE "HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and Organizational Security Policies described, respectively, in section 3.2 and 3.3 of the Security Target [ST] are complied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG]).

[2] Activities with the _HCDPP extension were entered by the lab to clearly organize the activities from the PP's "Assurance Activities" for each SFR and Appendixes E and F of [HCDPP].

# 9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

## 9.1 TOE delivery

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 which contains both the System firmware and the Jetdirect Inside firmware. The evaluated firmware versions have been already provided in Table 1.

The steps to perform download of the TOE files are provided in the following:

1. Request a username and password by sending an email to the following address: ccc-hp-enterprise-imaging-printing@hp.com.
2. Open the following URL in a web browser: https://h30670.www3.hp.com/portal/kiosk.
3. On the PPS KIOSK login page, enter the username and password obtained in step 1, then click Next.
4. Click the link for your printer in the Tools, products, and technologies section. An overview of the Common Criteria certification is displayed. Do not click Request at this point.
5. Click the Installation link. The Installation page containing information to securely download the .zip file containing the evaluated firmware and guidance documentation opens.
6. Confirm that the Installation page was downloaded securely by verifying the following:

- The text in the URL field starts with https://
- The host following the https:// prefix is within the hp.com domain.
- A locked padlock icon is displayed by the web browser.
- The web browser has not displayed any warnings related to the website's certificate.

Anything to the contrary indicates that the Installation page was not downloaded securely, in which case nothing on the page can be trusted. If the connection is secure, either save or print the Installation page. After downloading the .zip file, its integrity must be verified using the information in the Installation page.

7. After saving the Installation page, click "Request". A sign in page opens.
8. If you have HP sign-in credentials, enter your username and password, then click Sign In. If you do not have HP sign-in credentials, click the Don't have an account? Sign up link and complete the registration process. The Product specifications page opens after signing in.
9. Review and make any necessary changes in the Customer Information and Address sections.
10. Review and agree to the software license terms, then click Next. An electronic delivery receipt is sent to the email address associated with your HP account. The Software downloads and licenses page appears.
11. Click the Download link for the .zip file in the Software section.

In order to verify the integrity of the HP SW Depot download, there is a tool called DigitalVolcano Hash Tool (version 1.1.0.0) capable of generating SHA-256 hashes. The steps below were written specifically with the DigitalVolcano Hash Tool:

1. Launch the DigitalVolcano Hash Tool.
2. Select SHA-256 from the Hash Type drop-down menu.
3. Click the Select File(s) button in the Input Field section and browse to the .zip file. The DigitalVolcano Hash Tool generates a SHA-256 hash of the .zip file and displays it in the area labeled Last Hash.
4. Visually compare the SHA-256 hash generated in the previous step with the SHA-256 hash contained in the Installation page from the HP SW Depot. If the hashes match, then the .zip file has not been compromised. If the hashes don't match, then either an error occurred during the download or the .zip file on the server is not the same as the original. Try downloading the .zip file again and repeat the verification steps. If on the successive attempt the hashes still do not match, and you are certain that the download proceeded without any issues, send an email to ccc-hp-enterprise-imaging-printing@hp.com describing the comparison failure.

In addition, it is possible to check the integrity of the firmware "xxxxxxx.bdl", where "xxxxxxxx" indicates the firmware file name and ".bdl" is the file extension, using the hash string SHA-256 available in Table 6.

| Model | Firmware name | SHA-256 |
|---|---|---|
| HP ColorLaserJet Enterprise M751 | cljM751_fs5.7.1.1_2507252_046129.bdl | 91a9da92823ac9d6b75b8cbbbae73880d721291cd238b8513af19aad2aeced61 |
| HP Color LaserJet Managed E75245 | cljmE75245_fs5.7.1.1_2507252_046129.bdl | 5ee6cae2299bcc295fea15c7d6bac02b5b159944471f9b223596361c093eb49d |
| HP LaserJet Enterprise M610 files | ljM610_fs5.7.1.1_2507252_046110.bdl | 14536dfbcd38521ebf894043b0845ae959b2f570aaf0d95e15235803099bb300 |
| HP LaserJet Enterprise M611, M612 | jM611_M612_fs5.7.1.1_2507252_046110.bdl | f4ca13ec5485713b20b4dfe45dc1770f554a25a11f1bcdee0301b585c12d8236 |
| HP Color LaserJet Enterprise M856 | cljM856_fs5.7.1.1_2507252_046112.bdl | df3fbad099bbdd81fbe5fd3f72efbcd01523ffe28493fcfb48aee7fe6b63e33f |
| HP LaserJet Enterprise M507 | ljM507_fs5.7.1.1_2507252_046139.bdl | 32010925404e3265fb8c36a731a8a5f5acdb843690d8d6903027450fc6164123 |

Table 6 - SHA-256 hashes for firmware

The customer receives the hardware independent of the ZIP file. The evaluated hardware models, which are listed in Table 1, are either already on the customer's premise or must be obtained from HP. The user can use the following steps to verify that the TOE hardware has not been tampered with during the delivery:

- Inspect the cardboard box the TOE hardware was delivered in. Ensure the cardboard box contains the HP logo, has not been opened and resealed, the product information label is present, and no major physical damage exists.
- Inspect the contents of the cardboard box. Ensure all expected items have been delivered, the packaging the TOE hardware is contained in has not been tampered, and no missing or reapplied tape exists on the TOE hardware.

After that, the user can verify that the delivered TOE hardware is the correct model by taking the following steps:

- Verify the full product model name, serial number and product number in the order confirmation is consistent with the label on the cardboard box.
- Verify the invoice located in the cardboard box the TOE hardware was delivered in is consistent with the order confirmation.
- Verify the serial number and product number on the product label on the back of the TOE hardware is consistent with the order confirmation.

## 9.2 Identification of the TOE by the User

The TOE user can identify TOE components as described below:

- **Hardware**: the model name is marked on the front of the TOE hardware and the product number on the product label on the back.
- **Firmware**: the user can verify firmware version by checking the "Configuration Page" through the EWS administrative interface or using the Control Panel.
- **Guidance documentation**: the version number is printed in the documents.

## 9.3 Installation, configuration, and secure usage of the TOE

TOE installation, configuration and secure usage shall be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria Evaluated Configuration Guide for HP Document Scanners [CCECG] contains detailed information for the secure installation and configurationof the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

The Developer also provides user guides for each evaluated printer models. These additional documents are listed in Table 1-2 ("User guides") of [CCECG].

# 10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is "HP Color LaserJet Enterprise M856, HP LaserJet Enterprise M610/M611/M612, HP LaserJet Enterprise M507, HP Color LaserJet Enterprise M751, and HP Color LaserJet Managed E75245 printers with HP FutureSmart 5.7.1.1 Firmware", developed by HP, Inc.

The evaluated configuration of the TOE includes the hardware models and firmware versions listed in Table 1.

The physical boundary of the TOE is the physical boundary of the HCD product. Options and add-ons that are not security relevant, such as finishers, are not part of the evaluation but can be added to the TOE without any security implications.

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

- Only one Administrative Computer is used to manage the TOE.
- Third-party solutions must not be installed on the TOE.
- 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 stored jobs must be assigned a Job PIN or Job Encryption Password.
- Jetdirect Inside management via telnet and FTP must be disabled.
- HP 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 support personnel, must be disabled.
- Wireless functionality must be disabled:
    - Near Field Communication (NFC) must be disabled.
    - Bluetooth Low Energy (BLE) must be disabled.
    - Wireless Direct Print must be disabled.
    - Wireless station must be disabled.
- PJL device access commands must be disabled.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- Remote Control-Panel use is disallowed.

- Local Device Sign In accounts must not be created (i.e., only the built-in Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS) using IPsec:
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services
- Device Administrator Password must be set.
- Remote Configuration Password must not be set.
- OAUTH2 use is disallowed.
- SNMP over HTTP use is disallowed.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- Firmware updates through REST Web Services is disallowed.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- Smart Cloud Print must be disabled.
- FIPS-140 must be disabled.
- Partial clean functionality of the TOE is disallowed.

## 10.1 TOE operational environment

The following required components are part of the Operational Environment (refer also to section 1.4.1 of the Security Target [ST]):

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

The following optional components are part of the Operational Environment.

- Client computers network 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).
- The Server Message Block (SMB) remote file systems.
- A Simple Mail Transfer Protocol (SMTP) gateway.

# 11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level defined by the SARs included in the PP [HCDPP], such activities do not require the execution of functional tests by the Developer, but only independent functional tests and penetration tests by the Evaluators.

## 11.1 Test configuration

All testing activities have been carried out remotely from the LVS premises on the Virtual Test Laboratory (VTL) located at the Developer site in Boise, Idaho, USA. The Developer setup the test environment with the actual TOE models.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the Common Criteria Evaluated Configuration Guide [CCECG] and the Security Target [ST].

The Evaluators performed testing remotely by connecting to the test environment using Microsoft Remote Desktop (RDP) and the communication was protected using TLSv1.2.

All remote test activities have been carried out in accordance with the instructions provided by the Italian Certification Body in the Scheme Information Note 5/23 - Conditions for performing tests remotely in Common Criteria evaluations [NIS5].

## 11.2 Functional and independent tests performed by the Evaluators

The Security Target [ST] claims exact conformance to the PP [HCDPP], which defines test cases mapped to SFRs. The Evaluators performed both automated and manual test cases to fulfil the required tests, thereby also fulfilling the requirements for ATE_IND.1.

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly. They also verified that the test environment was properly set up by the Developer.

The Evaluators tested the physical TOE models listed in Table 7, thereby covering all system firmware versions, while a rationale for product equivalence for tested models has been described by LVS based on information provided by Developer.

| TOE model name | System firmware version |
|---|---|
| HP Color LaserJet Enterprise M751 | 2507252_046129 |
| HP LaserJet Enterprise M610 | 2507252_046110 |
| HP Color LaserJet Enterprise M856 | 2507252_046112 |
| HP LaserJet Enterprise M507 | 2507252_046139 |

Table 7 - TOE models tested

The Evaluators executed all required tests described in the PPs [HCDPP] and [HCDPP-ERR], and in the applicable NIAP Technical Decisions listed in section 2.1.1 of the Security Target [ST].

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

## 11.3 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same VTL and the same TOE models already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

Since an attack requires an attack surface, the Evaluators decided to examine if the TOE exposes such interfaces, i.e., open ports.

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

Evaluators, based on search result, compiled a table of potentially applicable vulnerabilities: based on the analysis, the evaluator determined there are no potential vulnerabilities in the TOE.

The Evaluators concludes that the TOE is resistant to an attack potential of Basic in its intended operating environment. No exploitable or residual vulnerabilities have been identified.