Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/21

(Certification No.)

Prodotto: *(Product)* **HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware**

Sviluppato da: *(Developed by)* **HP, Inc.**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

Conforme a: *(Conformant to)* **Protection Profile for Hardcopy Devices v1.0 +Errata #1**

(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)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 23 settembre 2021

Common Criteria

This page is intentionally left blank

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware

OCSI/CERT/ATS/13/2020/RC

Version 1.0

23 September 2021

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for 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	23/09/2021

2 Table of contents

3 Acronyms

AES Advanced Encryption Standard

AH Authentication Headers

BEV Border Encryption Value

BLE Bluetooth Low Energy

CBC Cipher Block Chaining

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DH Diffie-Hellman

DNS Domain Name System

DPCM Decreto del Presidente del Consiglio dei Ministri

DRBG Deterministic Random Bit Generator

DSA Digital Signature Algorithm

EAL Evaluation Assurance Level

ECB Electronic CodeBook

ECDH Elliptic-curve Diffie-Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

EEPROM Electrically Erasable Programmable Read-Only Memory

ESP Encapsulating Security Payload

ETR Evaluation Technical Report

EWS Exchange Web Services

FIPS Federal Information Processing Standards

FTP File Transfer Protocol

HCD Hardcopy Device

HMAC Keyed-Hash Message Authentication Code

HTTP	HyperText Transfer Protocol
HTTPS	HTTP over Secure Socket Layer
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
NTLM	New Technology LAN Manager
NTS	Network Time Service
OCSI	Organismo di Certificazione della Sicurezza Informatica
OXPd	Open Extensibility Platform device
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
PSK	Pre-shared Key
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SED	Self-encrypting Drive

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
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 Criteria and regulations

[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. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[NIS120] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/20 – Condizioni per l'effettuazione di test da remoto in valutazioni Common Criteria, versione 1.0, 6 aprile 2020

4.2 Technical documents

[CCECG] "Common Criteria Evaluated Configuration Guide for HP Document Scanners HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner", Edition 1, HP Inc., May 2021

[ETR] Final Evaluation Technical Report "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware", Version 1, atsec information security S.r.l., 3 September 2021

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

[HCDPP-ERR] Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

[ST] "HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target", Version 1.2, HP Inc., 24 August 2021

5 Recognition of the certificate

5.1 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] has been 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 assurance components selected.

6 Statement of certification

The Target of Evaluation (TOE) is the product “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware”, developed by HP, Inc.

The TOE is a hardcopy device (HCD), also known as a scanner, 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]. 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 v 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 product “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 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 review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware
Security Target	“HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target”, Version 1.2 [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, and 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-ERR]
Evaluation starting date	17 December 2020
Evaluation ending date	3 September 2021

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.

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 TOE is “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware” with the following elements:

- HP Digital Sender Flow 8500 fn2 Document Capture Workstation;
- HP ScanJet Enterprise Flow N9120 fn2 Document Scanner;
- Guidance Documentation.

The following firmware modules are included in the TOE:

- Jetdirect Inside firmware;
- System firmware.

All TOE models use the same Jetdirect Inside firmware version: JSI24110014.

The TOE includes the following System firmware versions:

1. 2411097_060492
2. 2411097_060482

Table 1 shows the HCD models and System firmware versions included in this evaluation.

Product family	Model	Product number	Option codes	System firmware version
HP ScanJet Enterprise Flow	N9120 fn2 Document Scanner	L2763A	#201	2411097_060492
HP Digital Sender Flow	8500 fn2 Document Capture Workstation	L2762A	#201	2411097_060482

Table 1 - TOE hardware and firmware reference

For a detailed description of the TOE, consult sect. 1.4 and sect. 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 human users. It performs the functions of scanning 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 the Windows Embedded CE 6.0 R3 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.

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. 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 protect unencrypted email up to the SMTP gateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

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

The TOE requires a DNS server, an NTS server, and a WINS server in the Operational Environment. The TOE connects to 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 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 one field-replaceable nonvolatile storage device. This storage device is a disk-based self-encrypting drive (SED) that is FIPS 140-2 validated.

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both firmware components work together to provide the security functionality for the TOE. They are two separate components but they both share the same operating system. The operating system is part of the System firmware.

7.3.2 TOE security features

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

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **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.

- **Data encryption (cryptography)**:

    - **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 crypto algorithms and key sizes: DH (P=2048, SHA2-256), DSA (L=2048, N=224; L=2048, N=256; L=3072, N=256), ECDH (P-256, SHA2-256; P-384, SHA2-384; P521, SHA2-512), ECDSA (P-256, P-384, P-521), RSA (2048 and 3072 bits), AES-CBC (128 and 256 bits), AES-ECB (256 bits), SHA-1, SHA2-256, SHA2-384, SHA2-512, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512.

    - **Drive-lock password**: for secure storage, all TOE models contain a one field-replaceable nonvolatile storage device. This storage device is a FIPS 140-2 validated, disk-based, self-encrypting drive (SED). The SED in the TOE uses a 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 (i.e., EEPROM) located inside the TOE. The CTR_DRBG(AES-256) uses the Advanced Encryption Standard-Counter (AES-CTR) algorithm.

- **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.

- **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. The table below 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

- **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:

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

- **Access control**: the TOE enforces access control on TSF data and User Data. Each piece of User Data is assigned ownership and access to the data is limited by the access control mechanism. The permission sets used to define roles also affect the access control of each user. The TOE contains one field-replaceable, FIPS 140-2 validated SED. Together with the drive-lock password, this SED ensures that the TSF Data and User Data on the drive is not stored as plaintext on the storage device.

- **Image Overwrite**: the TOE also supports the optional Image Overwrite function defined in the PP [HCDPP]. The PP limits the scope of this function to the field-replaceable nonvolatile storage device.

- **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.

- **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.

- **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 System 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 sect. 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-ERR]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected 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 3 September 2021 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 16 September 2021. 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 check regularly 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 Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 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 2 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
Tests	**Class ATE**	Pass
Independent testing - conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass

Assurance classes and components		Verdict
Vulnerability survey	AVA_VAN.1	Pass

Table 2 - Final verdicts for assurance requirements

8.2 Additional assurance activities

The Protection Profile for Hardcopy Devices [HCDPP] includes additional assurance activities that are 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 3 summarizes the final verdict of the PP assurance activities carried out by the LVS.

PP assurance activities		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 3 - Final verdicts for PP assurance activities

8.3 Recommendations

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

Potential customers of the product “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware” are suggested to properly understand the specific purpose of certification 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 sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and the Organizational Security Policies described, respectively, in sect. 3.2 and 3.3 of the Security Target [ST] are respected.

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, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG]).

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 are provided in Table 1.

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

The customer receives the hardware independently 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

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, initialization and secure usage of the TOE

TOE installation, configuration and operation should 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 initialization of 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 the specific evaluated printer models. These additional documents are listed in Table 1-2 (“User guides”) and Table 1-3 (“Hardware installation guides”) of [CCECG].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware”, developed by HP, Inc.

The evaluated configuration of the TOE includes the hardware models and firmware versions listed in sect. 7.3.

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 (see sect. 1.5.4.3 of the Security Target [ST]):

- 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.
- Device USB must be disabled.
- Host USB plug and play must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services 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 station 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 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.
- Internet Fax and LAN Fax must be disabled.
- Firmware updates through REST Web Services is disallowed.

10.1 TOE operational environment

The following required components are part of the TOE operational environment (see sect. 1.4.1 of the Security Target [ST]):

- A Domain Name System (DNS) server.
- A Network Time Service (NTS) server.
- One 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 TOE operational environment:

- Microsoft SharePoint.
- The following remote file systems:

  - File Transfer Protocol (FTP).
  - Server Message Block (SMB).
- 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).

All remote test activities have been carried out in accordance with the instructions provided by the Italian Certification Body in the Scheme Information Note 1/20 - Conditions for performing tests remotely in Common Criteria evaluations [NIS120].

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 fulfill 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 4, thereby covering all system firmware versions.

TOE Name (hardware models)	Jetdirect Inside firmware version	System firmware version
HP ScanJet Enterprise Flow N9120 fn2 Document Scanner	JSI24110014	2411097_060492
HP Digital Sender Flow 8500 fn2 Document Capture Workstation		2411097_060482

Table 4 - Tested TOE models

The Evaluators executed all required tests described in the PPs [HCDPP] and [HCDPP-ERR], and in the applicable NIAP Technical Decisions listed in sect. 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).

The Evaluators determined that only UDP port 500 (ISAKMP) is available outside of IPsec. This is the expected result.

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