CSEC

Swedish Certification Body for IT Security

Certification Report - HP YA HCDPP

Issue: 1.0, 2019-jun-14

Authorisation: Helén Svensson, Lead certifier , CSEC

SWEDAC ACKREDITERING
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The TOE is the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner.

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 ST claims conformance to:

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

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden and the developer's premises in Boise, Idaho, USA, and was completed on the 11th of April 2019.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation conforms both to the evaluation activities in the HCDPP and to evaluation assurance level EAL 1, augmented by ASE_SPD.1.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2018007
Name and version of the certified IT product	• HP Digital Sender Flow 8500 fn2 Document Capture Workstation System firmware versions 2406249_032755 Jetdirect Inside firmware version JSI24060306 • HP ScanJet Enterprise Flow N9120 fn2 Document Scanner System firmware versions 2406249_032756 Jetdirect Inside firmware version JSI24060306
Security Target Identification	HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target, Date 2019-03-28, Version 2.0

EAL	for CCRA and EA_MLA:
	Protection Profile for Hardcopy Devices v1.0 with Errata #1, including ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, and AVA_VAN.1
	for SOGIS:
	EAL 1 + ASE_SPD.1

Sponsor	HP Inc.
Developer	HP Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.22.3
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2019-06-14

3 Security Policy

The TOE provides the following security services:

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

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

3.1 Identification, authentication, and authorization to use HCD functions

The following table shows the Internal and External Authentication mechanisms supported by the TOE in the evaluated configuration and maps the mechanisms to the interfaces that use them.

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

3.2 Access control

The TOE enforces access control on TSF data and User Data. Each piece of User Data is assigned ownership and access to the data is limited by the access control mechanism. The 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.

The TOE also supports the optional Image Overwrite function (O.IMAGE_OVERWRITE) defined in [HCDPPv1.0]. [HCDPPv1.0] limits the scope of this function to the field-replaceable nonvolatile storage device.

3.3 Data encryption (a.k.a 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.

Drive-lock password

For secure storage, all TOE models contain a single FIPS 140-2 validated self-encrypting drive (SED) that is a field-replaceable nonvolatile storage device. This SED 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 (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 signed update images.

Digital signatures for TSF testing

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

3.4 Trusted communications

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

3.5 Administrative roles

The TOE supports administrative and non-administrative roles. Assignment to these roles is controlled by the TOE's administrator. In the case of the Control Panel, EWS, and RESTful (Windows Sign In) interfaces, the roles are implemented as permission sets. In the case of RESTful (Local Sign In) interface, only one administrative account exists.

3.6 Auditing

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

3.7 Trusted operation

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

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

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

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

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

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

4.2 Clarification of Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

5 Architectural Information

The TOE is designed to be shared by many human users. It performs the functions of scanning and sending 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 the Windows Embedded CE 6.0 R3 running on an Arm Cortex-A8 processor.

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

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

The Web Services (WS) interfaces allow administrators to externally manage the TOE. The evaluated configuration only supports the RESTful Web Services interface. The RESTful 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 (Flow models only) 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 disk drive. This drive is a FIPS 140-2 validated SED. Depending on the TOE model, this drive may come pre-installed or the TOE may require the installation of the HP High-Performance Secure Hard Disk assembly prior to deploying the TOE.

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both firmware components work together to provide the security functionality defined in this document for the TOE. They are shown as two separate components but they both share the same operating system. The operating system is part of the System firmware. The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the System firmware. The Jetdirect Inside firmware includes IPsec and the management functions for managing this network-related feature. It also provides the network stack and drivers controlling the TOE's embedded Ethernet interface. The System firmware controls the overall functions of the TOE from the Control Panel to the storage drive.

6 Documentation

The following guidance documents are available

- Preparatory Procedures and Operational Guidance for the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner [CCECG]
- HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide [8500_N9120-UG]
- HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide [8500_N9120-IG]

7 IT Product Testing

7.1 Evaluator Testing

Testing was performed at the developer's site in Boise, Idaho, USA. Both models of HCDs were included the testing.

The evaluator executed all required tests in [HCDPPv1.0].

All test results were the results expected.

7.2 Penetration Testing

Testing was performed at the developer's site in Boise, Idaho, USA.

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

The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec which was the expected result.

8 Evaluated Configuration

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

- HP Digital Sending Software (DSS) must be disabled.
- Only one Administrative Computer is used to manage the TOE.
- HP and third-party applications cannot be installed on the TOE.
- Type A and B USB ports must be disabled.
- Remote Firmware Upgrade through any means other than the EWS and USB must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Full Authentication must be enabled (this disables the Guest role).
- SNMPv1/v2 and SNMPv3 must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- Near Field Communication (NFC) must be disabled.
- Wireless networking (WLAN) must be disabled.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS):
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services

9 Results of the Evaluation

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

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

The evaluators overall verdict is PASS.

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

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

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

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

10 Evaluator Comments and Recommendations

None.

11 Glossary

AES	Advanced Encryption Standard
AH	Authentication Header (IPsec)
Arm	Advanced RISC Machine
BEV	Border Encryption Value
CC	Common Criteria
Cert	certificate
cPP	Collaborative Protection Profile
CSEC	The Swedish Certification Body for IT Security
CTR	Counter mode
CTR_DRBG	Counter mode DRBG
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSS	Digital Sending Software
EAL	Evaluated Assurance Level
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
FIPS	Federal Information Processing Standard
HCD	Hardcopy Device
HCDPP	Hardcopy Device Protection Profile
HP	Hewlett-Packard
IKE	Internet Key Exchange (IPsec)
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
OSP	Organizational Security Policy
OXP	Open Extensibility Platform
OXPd	OXP device layer
KCS	Public-Key Cryptography Standards
PP	Protection Profile
PSK	Pre-Shared Key
REST	Representational State Transfer (a.k.a. RESTful)
RESTful	See REST
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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WS	Web Services

12 Bibliography

ST HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target, Date 2019-03-28, Version 2.0

CCECG Preparatory Procedures and Operational Guidance for the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner

8500_N9120-UG HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide

8500_N9120-IG HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide

HCDPPv1.0 Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP, 2015-09-10, Version 1.0

ERRATA Protection Profile for Hardcopy Devices - v1.0, Errata #1, June 2017

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2019-01-21, document version 30.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2019-01-16, document version 8.0

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

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

QMS 1.21.5 valid from 2018-11-19

QMS 1.22 valid from 2019-02-01

QMS 1.22.1 valid from 2019-03-08

QMS 1.22.2 valid from 2019-05-02

QMS 1.22.3 valid from 2019-05-20

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

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.22.3”. The certifier concluded that, from QMS 1.21.5 to the current QMS 1.22.3, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs