Swedish Certification Body for IT Security

Certification Report - HP NAMS HCDPP

Issue: 1.0, 2019-feb-12

Authorisation: Jerry Johansson, Lead certifier , CSEC

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

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a single function printer (SFP). The following model series are included in the scope of the evaluation:

HP PageWide Enterprise Color Printer 556,

HP LaserJet Enterprise Printer M607/M608/M609,

HP LaserJet Managed Printer E60055/E60065/E60075,

HP PageWide Enterprise Color Printer 765,

HP PageWide Managed Color Printer E75160,

HP LaserJet Enterprise Color Printer M652/M653,

HP LaserJet Managed Color Printer E65050/E65060

These SFPs provide network printing and storing. The evaluated security features include administrator and user identification and authentication, encrypted network communication (IPSec), encrypted storage of files etc.

The ST claims conformance to the Protection Profile for Hardcopy Devices v1.0, Errata #1, TD0157, TD0176, TD0219, and TD0261. TD0074, TD0253, TD0299 are not applicable. The evaluation has verified exact conformance to the PP.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, to some extent in the approved foreign location in Austin, Texas, USA, and the developer's premises in Boise, Idaho, USA, and was completed on the 30th of January 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.

atsec information security AB is a licensed evaluation facility for Common Crite-ria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation re-sults confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for the evaluation assurance level EAL 1 + ASE_SPD.1 as well as the evaluation activities in HCDPP.

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	CSEC2017012
Name and version of the certified IT product	HP PageWide Enterprise Color Printer 556, System firmware version 2406249_032769 JDI firmware version JSI24060306 HP LaserJet Enterprise Printer M607/M608/M609, System firmware version 2406249_032768 JDI firmware version JSI24060306 HP LaserJet Managed Printer E60055/E60065/E60075, System firmware version 2406249_032768 JDI firmware version JSI24060306 HP PageWide Enterprise Color Printer 765 System firmware version 2406249_032751 JDI firmware version JSI24060306 HP PageWide Managed Color Printer E75160 System firmware version 2406249_032751 JDI firmware version JSI24060306 HP LaserJet Enterprise Color Printer M652/M653, System firmware version 2406249_032761 JDI firmware version JSI24060306 HP LaserJet Managed Color Printer E65050/E65060 System firmware version 2406249_032761 JDI firmware version JSI24060306
Security Target	HP PageWide Enterprise Color Printer 556, HP LaserJet Enterprise Printer M607/M608/M609, HP LaserJet Managed Printer E60055/E60065/E60075, HP PageWide Enterprise Color Printer 765 HP PageWide Managed Color Printer E75160 HP LaserJet Enterprise Color Printer M652/M653, HP LaserJet Managed Color Printer E65050/E65060 Security Target

Assurance packages	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
Scheme Notes Release	1.22
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2019-02-12

3 Security Policy

The TOE provides the following security services:

- Identification, Authentication, and Authorization
- Access Control
- Cryptography
- Trusted Communications
- Administrative Roles
- Auditing
- Trusted Operation
- Data Clearing

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

The TOE supports user accounts in the local device (in the evaluated configuration only for administrators), for Control Panel, EWS and RESTful users. SNMPv3 users also uses the local user account database. All other users have to use external authentication via LDAP or a Windows Domain Server.

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.

3.3 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 and between the TOE and client computers. IPsec provides assured identification of the endpoints. It implements IKEv1 and transport mode. The TOE also supports both X.509v3 certificates and pre-shared keys (PSKs) for endpoint authentication.

3.5 Administrative Roles

The TOE supports roles implemented as permission sets. The administrator assigns users to these roles. The SNMPv3 and RESTful interfaces are only accessible to administrators.

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.

3.8 Data Clearing

The TOE also supports the Image Overwrite function (O.IMAGE_OVERWRITE) defined in [HCDPP] for the field-replaceable nonvolatile storage device.

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 the HCD a.k.a. 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).

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 SNMP network interface allows administrators to remotely manage the TOE using external SNMP-based management tools. The evaluated configuration supports SNMPv3 only. 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.

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

The TOE protects all network communications with Internet Protocol Security (IPsec). Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using PSK or X.509v3 certificates. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported into the TOE with the CA certificate.

Because IPsec authenticates the computers (not the individual users of the computer), access to the Administrative Computer should be restricted to TOE administrators only.

The TOE distinguishes between the Administrative Computer and Network Client Computers by using IP addresses, IPsec, and the embedded Jetdirect Inside's internal firewall. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one and the Device Administrator Password must be set.

Each HCD contains a user interface (UI) called the Control Panel. Depending on the SFP model, the Control Panel contains either a non-touchscreen LCD or a touchscreen LCD. On SFP models that contain a Control Panel with a non-touchscreen LCD, the Control Panel also contains a physical keypad. 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.

6 Documentation

For proper configuration of the TOE into the evaluated configuration, the following guidance documents are available:

CCECG	Preparatory Procedures and Operational Guidance for HP Single-Function Printers
556 UG	HP PageWide Enterprise Color 556 User Guide
556 IG	HP PageWide Enterprise Color 556 Installation Guide
607/8/9 UG	HP LaserJet Enterprise M607, M608, M609 User Guide
607/8/9 IG	HP LaserJet Enterprise M607, M608, M609 Installation Guide
765 UG	HP PageWide Enterprise Color 765, HP PageWide Color 755 User Guide
765 IG	HP PageWide Enterprise Color 765 series HP PageWide Color 755 series Installation Guide
E75160 UG	HP PageWide Managed Color E75160, P75250 User Guide
E75160 IG	HP PageWide Managed Color E75160 Series HP PageWide Managed Color P75250 Series Installation Guide
M652/3 UG	HP Color LaserJet Enterprise M652, M653 User Guide
M652 IG	HP Color LaserJet Enterprise M652 Installation Guide
M653 IG	HP Color LaserJet Enterprise M653 Installation Guide

7 IT Product Testing

7.1 Evaluator Testing

The evaluators have performed all required tests listed in the HCDPP and have tested a selection of MFP models covering each firmware combination. The testing was performed at the developer site in Boise, Idaho.

The evaluator testing also covers the requirements of ATE_IND.1.

All test results were as expected.

7.2 Penetration Testing

The evaluator examined all potential interfaces (UDP and TCP ports), for IP v4 and for IP v6. The testing was performed at the developer site in Boise, Idaho, USA.

The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec.

All test results were as expected.

8 Evaluated Configuration

The TOE firmwares run on top of Windows Embedded CE 6.0 R3 on Arm Cortex-A8

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

- 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 (e.g., PJL) and USB must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- File System External Access must be disabled.
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Full Authentication must be enabled (this disables the Guest role).
- SNMP support is limited to SNMPv3.
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- Bluetooth Low Energy (BLE) must be disabled.
- Wireless networking (WLAN) must be disabled.
- PJL device access commands must be disabled.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS):
  - 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 [1] 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

[1] State the level of attack potential that is applicaple.

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

BEV	Border Encryption Value
CC	Common Critera
CSEC	The Swedish Certification Body for IT Security
DNS	Domain Name System
EAL	Evaluated Assurance Level
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
GUI	Graphical User Interface
HCD	Hardcopy Device
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IKE	Internet Key Exchange (IPsec)
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer
NTS	Network Time Service
OS	Operating System
OXP	Open Extensibility Platform
OXPd	OXP device layer
PJL	Printer Job Language
PP	Protection Profile
PSTN	Public Switched Telephone Network
REST	Representational State Transfer (a.k.a. RESTful)
RESTful	See REST
SED	Self-Encrypting Drive
SFP	Single Function
SHA	Secure HashAlgorithm
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
WS	Web Services

12 Bibliography

ST — HP PageWide Enterprise Color Printer 556,
HP LaserJet Enterprise Printer M607/M608/M609,
HP LaserJet Managed Printer E60055/E60065/E60075,
HP PageWide Enterprise Color Printer 765
HP PageWide Managed Color Printer E75160
HP LaserJet Enterprise Color Printer M652/M653,
HP LaserJet Managed Color Printer E65050/E65060
Security Target, HP Inc., 2019-01-29, document version 1.33

CCECG — Preparatory Procedures and Operational Guidance for HP Single-Function Printers
HP PageWide Enterprise Color Printer 765,
HP PageWide Managed Color Printer E75160
HP LaserJet Enterprise Color Printer M652/M653,
HP LaserJet Managed Color Printer E65050/E65060
HP LaserJet Enterprise Printer M607/M608/M609,
HP LaserJet Managed Printer E60055/E60065/E60075,
HP PageWide Enterprise Color Printer 556,
HP Inc., 2018-11-28, document version: Edition 1, 11/2018

556 UG — HP PageWide Enterprise Color 556 User Guide, HP Inc., 2016-05, document version 1

556 IG — HP PageWide Enterprise Color 556 Installation Guide, HP Inc., (2018-11-29)

60X UG — HP LaserJet Enterprise M607, M608, M609 User Guide, HP Inc., 2017-08, document version 2

60X IG — HP LaserJet Enterprise M607, M608, M609 Installation Guide, HP Inc., (2018-11-29)

765 UG — HP PageWide Enterprise Color 765, HP PageWide Color 755 User Guide, HP Inc., 2017-05, document version 1

765 IG — HP PageWide Enterprise Color 765 series HP PageWide Color 755 series Installation Guide, HP Inc., (2018-11-29)

E75160 UG — HP PageWide Managed Color E75160, P75250 User Guide,

HP Inc., 2018-03, document version 2

E75160 IG — HP PageWide Managed Color E75160 Series HP PageWide Managed Color P75250 Series Installation Guide, HP Inc., (2018-11-29)

M652/3 UG — HP Color LaserJet Enterprise M652, M653 User Guide, HP Inc., 2017-05, document version 1

M652 IG — HP Color LaserJet Enterprise M652 Installation Guide, HP Inc., (2018-11-29)

M653 IG — HP Color LaserJet Enterprise M653 Installation Guide, HP Inc., (2018-11-29)

HCDPP — Protection Profile for Hardcopy Devices, IPA/NIAP/MFP TC, 2015-09-10, document version 1.0

ERRATA — Protection Profile for Hardcopy Devices - v1.0 Errata#1 June 2017, IPA/NIAP/HCD TC, 2017-06, 27 February 2015, version 1.0

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

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

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

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 project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2017-08-30:

QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13
QMS 1.21.5	valid from 2018-11-19
QMS 1.22	valid from 2019-02-01

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" and "Ändringslista CSEC QMS 1.21.5".

The certifier concluded that, from QMS 1.20.5 to the current QMS 1.22, there are no changes with impact on the result of the certification.