Ärendetyp: 6
Diarienummer: 19FMV4376-30:1
Dokument ID 7DFAYPHQVZ4V-1834444990-2324

Swedish Certification Body for IT Security

Certification Report - HP GIFF 2600PP

Issue: 1.0, 2020-Dec-08

Authorisation: Ulf Noring, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the HP FutureSmart 4.8 firmware, and guidance documentation, for the following printer models:

HP LaserJet Enterprise MFP M528
HP LaserJet Managed MFP E52645
HP LaserJet Managed MFP E82540/E82550/E82560
HP LaserJet Managed MFP E72425/E72430
HP LaserJet Managed MFP E62655/E62665/E62675
HP Color LaserJet Managed MFP E87640/E87650/E87660
HP Color LaserJet Managed MFP E77422/E77428
HP Color LaserJet Managed MFP E67650/E67660

The TOE consists of the contents of the firmware with the exception of the operating system which is part of the Operational Environment.

The TOE contains functions for copying, printing, faxing, scanning, storing, and retrieving of documents through the above mentioned MFP models.

The firmware and guidance documentation are packaged in a single ZIP file and available for download from the HP Inc. website. 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 ST claims demonstrable conformance to the IEEE Std 2600.1-2009 Protection Profile for Hardcopy Devices, Operational Environment A, v1.0 [PP2600A], including the CPY, DSR, FAX, PRT, SCN and SMI packages.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden and to some extent in the developer's premises in Boise, Idaho, USA, and was completed on the 28th of October 2020.

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 to evaluation assurance level

EAL 3, augmented by ALC_FLR.2.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Critera Evaluation and Certification Scheme. atsec information security AB 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 results 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 3 + ALC_FLR.2.

The technical information in this report is based on the Security Target [ST] produced by HP Inc. and the Final Evaluation Technical Report [FER] produced by atsec information security AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. 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.

As specified in the security target of this evaluation, the invocation of cryptographic primitives has been included in the TOE, while the implementation of these primitives has been located in TOE environment. Therefore the invocation of cryptographic primitives has been in the scope of this evaluation, while correctness of implementation of cryptographic primitives has been excluded from the TOE. Correctness of implementation is done through third party certification Cryptographic Algorithm Validation Program (CAVP) certificates DSA #1432, CVL #1999, AES #5567, RSA #2996, SHS #4474, HMAC #3711 and DRBG #2220 referred to in table 49 in the Security Target.

Users of this product are advised to consider their acceptance of this third party affirmation regarding the correctness of implementation of the cryptographic primitives.

2 Identification

Certification Identification	
Certification ID	CSEC2019016
Name and version of the certified IT Product	HP FutureSmart 4.8 firmware for the MFP model series mentioned at the bottom of this page.
Security Target Identification	HP LaserJet Enterprise MFP M528, HP LaserJet Managed MFP E52645, HP LaserJet Managed MFP E82540 / E82550 / E82560, HP LaserJet Managed MFP E72425 / E72430, HP LaserJet Managed MFP E62655 / E62665 / E62675, HP Color LaserJet Managed MFP E87640 / E87650 / E87660, HP Color LaserJet Managed MFP E77422 / E77428, HP Color LaserJet Managed MFP E67650 / E67660 Security Target, HP Inc., 23 October 2020, version 1.55
EAL	EAL 3 + ALC_FLR.2
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	1.23.2
Scheme Notes Release	16.0
Recognition Scope	CCRA, SOGIS, EA MLA
Certification date	2020-12-08

Certified product versions (system firmware, model series):
2408067_049142, HP LaserJet Enterprise MFP M528
2408067_049142, HP LaserJet Managed MFP E52645
2408067_049168, HP LaserJet Managed MFP 82540/E82550/E82560
2408067_049145, HP LaserJet Managed MFP E72425/E72430
2408067_049150, HP LaserJet Managed MFP E62655/E62665/E62675
2408067_049159, HP Color LaserJet Managed MFP E87640/E87650/E87660
2408067_049161, HP Color LaserJet Managed MFP E77422/E77428
2408067_049166, HP Color LaserJet Managed MFP E67650/E67660

All TOE models use the same Jetdirect Inside firmware version:
JSI24080014

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptography
- Identification and Authentication
- Data Protection and Access Control
- Protection of the TSF
- TOE Access Protection
- Trusted Channel Communication and Certificate Management
- User and Access Management

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

3.1 Auditing

The TOE performs auditing of document-processing functions and security-relevant events. Both the Jetdirect Inside and HCD System firmware generate audit records. The TOE connects and sends audit records to a syslog server for long-term storage and audit review. (The syslog server is part of the Operational Environment.)

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The HP FutureSmart QuickSec 5.1 (a.k.a. QuickSec) cryptographic library within the TOE is used to supply the cryptographic algorithms for IPsec.

The TOE supports key derivation and decryption for printing encrypted stored print jobs. Both the key derivation function and decryption algorithm used by the TOE for printing encrypted stored print jobs are included in the TOE.

The TOE contains a Data Integrity Test that provides administrators the ability to verify the integrity of specific TSF Data on-demand through the EWS. The Data Integrity Test uses the SHA-256 algorithm to verify the integrity of TSF Data. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA2-256 algorithm.

The TOE contains a Code Integrity Test that provides administrators the ability to verify the integrity of TOE executable code files stored on the primary storage drive on-demand through the EWS. The Code Integrity Test uses the SHA-256 algorithm to verify the integrity of TOE executable code files. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937, which is part of the operational environment, supplies the SHA2-256 algorithm.

There is also some cryptography in the MFP models that is outside of the scope of the TOE. Some MFP models contain one or two disk-based self-encrypting drives. In those cases the encryption is completely transparent to the TOE. For MFP models that use eMMC storage as the primary storage drive, certain areas of the eMMC are encrypted by the TOE using the MFP hardware, but that encryption is not claimed as a security function in the ST and has thus not been evaluated.

3.3 Identification and Authentication

● Control Panel

The Control Panel supports both local and remote sign-in methods. For local sign-in, only the built-in Device Administrator account can be used in the evaluated configuration. For remote sign-in, LDAP and Windows (via Kerberos) sign in are supported.

All users must sign in prior to being allowed to access any protected Control Panel applications and features.

When users sign in through the Control Panel, the TOE displays dots for each character of access code or password typed to prevent onlookers from viewing another user's authentication data. The TOE also contains account lockout functionality for the built-in Device Administrator account to help prevent password discovery through a brute-force attack.

● IPsec

The TOE uses IP addresses and RSA X.509v3 certificates via the IKE protocol (IKEv1 and IKEv2) to identify and authenticate client computers and other trusted IT products (e.g. Kerberos server). The TOE's internal firewall maintains lists (IPsec/Firewall address templates) of IP addresses of client computers that can connect to the TOE. Mutual identification and authentication must be completed before any tasks can be performed by a client computer.

3.4 Data Protection and Access Control

The TOE controls user access to functions available at the Control Panel using permissions. Each Control Panel application and protected feature has an associated permission. A permission is configured to either grant or deny access. Permissions are defined in Permission Sets (a.k.a. User Roles) which are assigned to users. To execute a Control Panel application or protected feature, the applicable permission must be configured to grant access in the Permission Set applied to a user.

Users control access to print (non-encrypted) and copy jobs that they place in Job Storage by assigning Job PINs to these jobs.

The TOE can store and decrypt encrypted stored print jobs received from a client computer that has the HP Universal Printer Driver installed. A stored print job is first encrypted by the client computer and protected with a user-specified Job Encryption Password. The job is sent encrypted to the TOE and stored encrypted by the TOE.

To print or delete an encrypted stored print job at the Control Panel, a non-administrative user must provide the correct Job Encryption Password for the encrypted stored print job. An administrative user can delete an encrypted stored print job at the Control Panel without providing a Job Encryption Password but must provide the correct Job Encryption Password to print the job.

3.5 Protection of the TSF

The TOE contains a suite of self tests to test specific security functionality of the TOE.

It contains data integrity checks for testing specific TSF Data of the TOE and for testing the stored TOE executables.

The TOE contains a system clock that is used to generate reliable timestamps. In the evaluated configuration, the TOE must be configured to synchronize its system clock with a Network Time Protocol (NTP) server.

3.6 TOE Access Protection

The TOE supports an inactivity timeout for Control Panel sessions. If a logged in user is inactive for longer than the specified period, the user is automatically logged off of the TOE.

3.7 Trusted Channel Communication and Certificate Management

The TOE uses IPsec as means to provide trusted channel communications. IPsec uses X.509v3 certificates, the Internet Security Association and Key Management Protocol (ISAKMP), IKEv1, IKEv2 and Encapsulating Security Payload (ESP) to protect communications.

The IPsec and IKE cryptographic algorithms are all supplied by the QuickSec cryptographic library. The QuickSec cryptographic library is part of the Operational Environment, but the TOE controls the usage of these algorithms.

In addition, the TOE provides certificate management functions used to manage (add, replace, delete) X.509v3 certificates.

3.8 User and Access Management

Only administrators have the authority to manage the security functionality of the TOE. They can manage the Administrator Access Code, IPsec certificates, IPsec/Firewall address templates, service templates and rules, sign-in policy, and the system clock.

Normal users can only manage user data that they have access to on the TOE.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

A.ACCESS.MANAGED

The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

A.ADMIN.PC.SECURE

The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it.

A.USER.PC.POLICY

User computers are configured and used in conformance with the organization's security policies.

A.USER.TRAINING

TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

A.ADMIN.TRAINING

Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. The organization security policies and procedures include security awareness training covering topics such as how to identify and avoid clicking on malicious links.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

A.SERVICES.RELIABLE

When the TOE uses any of the network services DNS, Kerberos, LDAP, NTP, SMTP, syslog, SMB, SharePoint, and/or WINS, these services provide reliable information and responses to the TOE.

A.EMAILS.PROTECTED

For emails received by the SMTP gateway from the TOE, the transmission of emails between the SMTP gateway and the email’s destination is protected.

4.2 Clarification of Scope

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

T.DOC.DIS

User Document Data may be disclosed to unauthorized persons.

T.DOC.ALT

User Document Data may be altered by unauthorized persons.

T.FUNC.ALT

User Function Data may be altered by unauthorized persons.

T.PROT.ALT

TSF Protected Data may be altered by unauthorized persons.

T.CONF.DIS

TSF Confidential Data may be disclosed to unauthorized persons.

T.CONF.ALT

TSF Confidential Data may be altered by unauthorized persons.

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

P.USER.AUTHORIZATION

To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION

To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING

To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT

To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

P.ADMIN.PASSWORD

To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that it is required to perform security-relevant actions through the EWS and at the Control Panel.

P.USERNAME.CHARACTER_SET

To prevent ambiguous user names in the TOE's audit trail, the user names of the LDAP and Windows Sign In users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

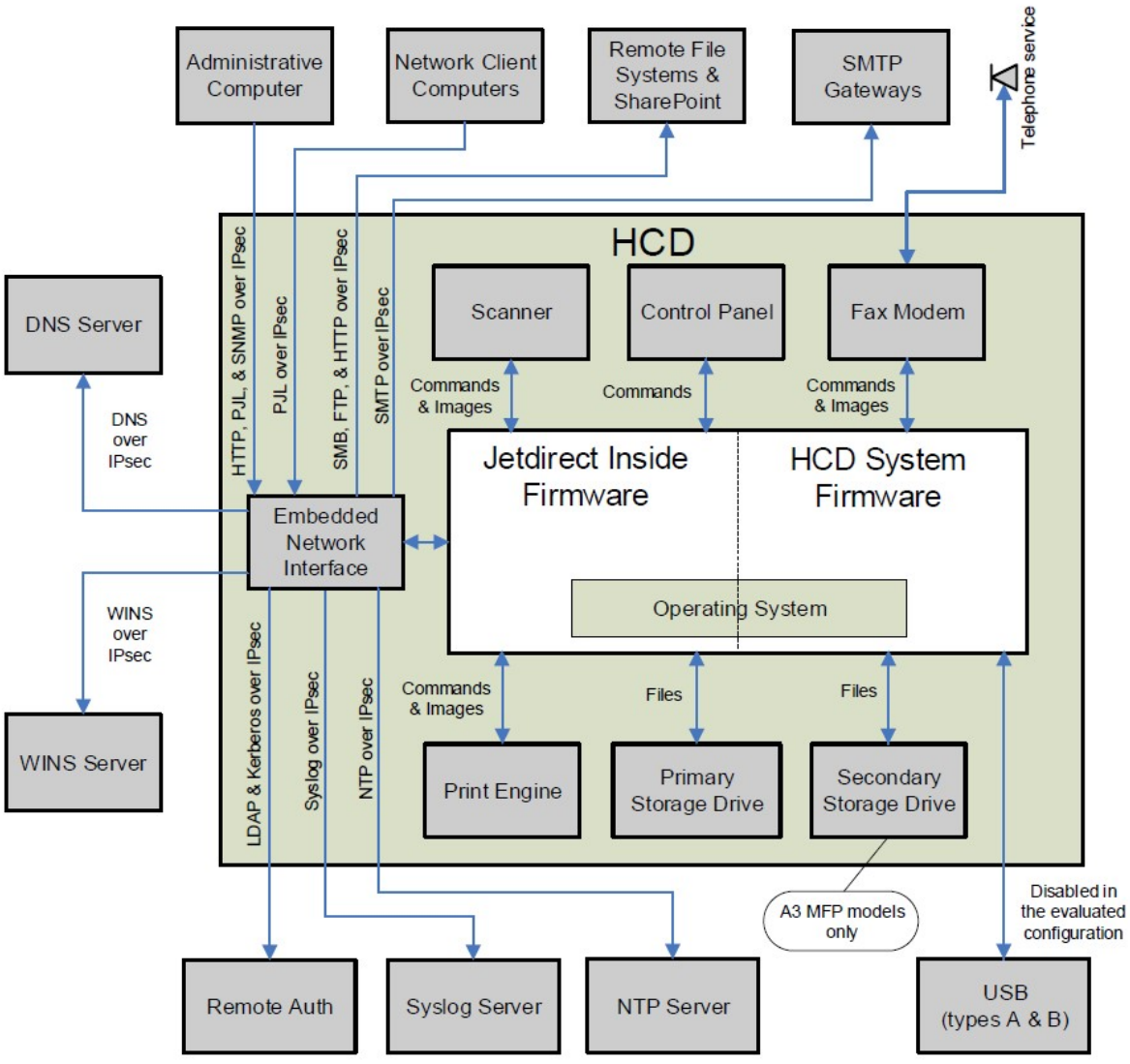
P.REMOTE_PANEL.DISALLOWED

To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature.

5 Architectural Information

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

In the diagram below, the unshaded parts show the Firmware parts that constitute the TOE.



The Security Target [ST] contains further descriptions of the product components and the TOE.

6 Documentation

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

CCECG	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP LaserJet Enterprise MFP M528, HP LaserJet Managed MFP E52645, HP LaserJet Managed MFP E82540 / E82550 / E82560, HP LaserJet Managed MFP E72425 / E72430, HP LaserJet Managed MFP E62655 / E62665 / E62675, HP Color LaserJet Managed MFP E87640 / E87650 / E87660, HP Color LaserJet Managed MFP E77422 / E77428, HP Color LaserJet Managed MFP E67650 / E67660
E825_E876-UG	HP LaserJet Managed MFP E82540du, E82550du, E82560du HP Color LaserJet Managed MFP E87640du, E87650du, E87660du User Guide
E825-IG	HP LaserJet Managed Flow MFP E82540-E82560 Engine Install Guide
E876-IG	HP Color LaserJet Managed Flow MFP E87640-E87660 Engine Install Guide
E77422_8-UG	HP Color LaserJet Managed MFP E77422, E77428 User Guide
E77422_8-IG	HP Color LaserJet Managed MFP E77422, E77428 Engine Install Guide
E72425_30-UG	HP LaserJet Managed MFP E72425, E72430 User Guide
E72425_30-IG	HP LaserJet Managed MFP E72425, E72430 Engine Install Guide
E62655_65_75-UG	HP LaserJet Managed MFP E62655, E62665, HP LaserJet Managed Flow MFP E62665, E62675 User Guide
E62655_65_75-IG	HP LaserJet Managed MFP E62655, E62665, HP LaserJet Managed Flow MFP E62665, E62675 Installation Guide
E67650_60-UG	HP Color LaserJet Managed MFP E67650 HP Color LaserJet Managed Flow MFP E67660 User Guide
E67650_60-IG	HP Color LaserJet Managed MFP E67650, E67660 Installation Guide

M528-UG	HP LaserJet Enterprise MFP M528 HP LaserJet Enterprise Flow MFP M528
M528-IG	HP LaserJet Enterprise MFP M528 Install Guide
E52645-UG	HP LaserJet Managed MFP E52645 HP LaserJet Managed Flow MFP E52645 User Guide
[E52645-IG]	HP LaserJet Enterprise MFP E52645 Install Guide

7 IT Product Testing

7.1 Developer Testing

Except for the IPSec tests, the developers tested the TOE on seven hardware models, both automatically and manually. IPSec tests were run on one hardware model. The developer tests cover all TSFI, all SFRs and all subsystems. All test results were as expected. Testing was performed by the developer at the HP site in Boise, Idaho, USA.

7.2 Evaluator Testing

The evaluators tested the TOE by running automated tests on three hardware models, and manual tests on three other models. IPSec tests were run on two hardware models.

The evaluators re-ran a sample of the developer tests, designed to cover all SFR-enforcing and SFR-supporting TSFIs and subsystems. All test results were as expected. The evaluators' testing was performed remotely from the evaluators' own premises in Stockholm, Sweden. The remote location for the evaluators' tests was the developer site in Boise, Idaho, USA.

7.3 Penetration Testing

The evaluators penetration tested the TOE on three hardware models. They examined all potential interfaces (UDP and TCP ports), i.e., all IPv4 and IPv6 UDP and TCP ports. The results of the port scan indicate that only UDP port 500 (ISAKMP) is open, and that all other ports are only accessible upon establishing an IPsec connection, which is in line with the expected outcome.The evaluators' testing was performed remotely from the evaluators' own premises in Stockholm, Sweden. The remote location for the evaluators' tests was the developer site in Boise, Idaho, USA.

8 Evaluated Configuration

The following items need to be adhered to in the evaluated configuration:

• HP Digital Sending Software (DSS) must be disabled

• Device Administrator Password must be set as per P.ADMIN.PASSWORD

• Remote Configuration Password must not be set

• Only one Administrative Computer is used to manage the TOE

• Third-party solutions are not installed on the TOE

• All non-fax stored jobs must be assigned a Job PIN or Job Encryption Password

• All received faxes must be converted into stored faxes

• Fax Archive must be disabled

• Fax Forwarding must be disabled

• Fax polling receive must be disabled

• Internet Fax and LAN Fax must be disabled

• PC Fax Send must be disabled

• Device USB and Host USB plug and play must be disabled

• Firmware upgrades sent as print jobs through P9100 interface must be disabled

• Jetdirect Inside management via telnet and FTP must be disabled

• Jetdirect XML Services must be disabled

• PJL Drive Access and PS Drive Access must be disabled

• IPsec authentication using X.509v3 certificates must be enabled (IPsec authentication using Kerberos or Pre-Shared Key is not supported)

• IPsec Authentication Headers (AH) must be disabled

• Device Guest permission set's permissions must be configured to deny access (this disables the Guest role)

• SNMP support limited to:

  o SNMPv1/v2 read-only

  o SNMPv3

• SNMP over HTTP use is disallowed

• OAuth use is disallowed

• 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

• Bluetooth Low Energy (BLE) must be disabled

• Wireless Direct Print must be disabled

• Wireless station capabilities must be disabled

• PJL device access commands must be disabled

• User names for the LDAP and Windows Sign In users must only contain the characters defined in P.USERNAME.CHARACTER_SET

• Remote Control-Panel use is disallowed per P.REMOTE_PANEL.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):
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services
- HP JetAdvantage Link Platform must be disabled
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration

9 Results of the Evaluation

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

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

The evaluators' overall verdict is PASS.

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

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional specification	ADV_FSP.3	PASS
TOE design	ADV_TDS.2	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC	PASS
CM capabilities	ALC_CMC.3	PASS
CM scope	ALC_CMS.3	PASS
Delivery	ALC_DEL.1	PASS
Development security	ALC_DSV.1	PASS
Flaw remediation	ALC_FLR.2	PASS
Life-cycle definition	ALC_LCD.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	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS

Depth	ATE_DPT.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

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
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
LDAP	Lightweight Directory Access Protocol
MFP	Multi Function Printer
NTP	Network Time Protocol
OS	Operating System
PJL	Printer Job Language
PP	Protection Profile
REST	Representational State Transfer (a.k.a. RESTful)
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UDP	User Datagram Protocol
WS	Web Services

12 Bibliography

12.1 General

CC Combination of CCp1, CCp2, CCp3, and CEM (see below)

CCp1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3 Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

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

ST HP LaserJet Enterprise MFP M528, HP LaserJet Managed MFP E52645, HP LaserJet Managed MFP E82540 / E82550 / E82560, HP LaserJet Managed MFP E72425 / E72430, HP LaserJet Managed MFP E62655 / E62665 / E62675, HP Color LaserJet Managed MFP E87640 / E87650 / E87660, HP Color LaserJet Managed MFP E77422 / E77428, HP Color LaserJet Managed MFP E67650 / E67660 Security Target, HP Inc., 2020-10-23, document version 1.55

PP2600A 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, IEEE Computer Society, 12 June 2009, version 1.0

SP-002 SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2019-09-25, document version 9.0

12.2 Documentation

CCECG Common Criteria Evaluated Configuration Guide for HP Multifunction Printers
HP LaserJet Enterprise MFP M528,
HP LaserJet Managed MFP E52645,
HP LaserJet Managed MFP E82540 / E82550 / E82560,
HP LaserJet Managed MFP E72425 / E72430,
HP LaserJet Managed MFP E62655 / E62665 / E62675,
HP Color LaserJet Managed MFP E87640 / E87650 / E87660,
HP Color LaserJet Managed MFP E77422 / E77428,
HP Color LaserJet Managed MFP E67650 / E67660

HP Inc., 5/2020, Edition 11

E825_E876-UG HP LaserJet Managed MFP E82540du, E82550du, E82560du
HP Color LaserJet Managed MFP E87640du, E87650du, E87660du

	User Guide, HP Inc., 2/2019 Edition 2
E825-IG	HP LaserJet Managed Flow MFP E82540-E82560 Engine Install Guide, HP Inc., 2019
E876-IG	HP Color LaserJet Managed Flow MFP E87640-E87660 Engine Install Guide, HP Inc., 2019
E77422_8-UG	HP Color LaserJet Managed MFP E77422, E77428 User Guide, HP Inc., 4/2019, Edition 1
E77422_8-IG	HP Color LaserJet Managed MFP E77422, E77428 Engine Install Guide, HP Inc., 2019
E72425_30-UG	HP LaserJet Managed MFP E72425, E72430 User Guide, HP Inc., 4/2019, Edition 1
E72425_30-IG	HP LaserJet Managed MFP E72425, E72430 Engine Install Guide, HP Inc., 2019
E62655_65_75-UG	HP LaserJet Managed MFP E62655, E62665, HP LaserJet Managed Flow MFP E62665, E62675 User Guide, HP Inc., 04/2019, Edition 1
E62655_65_75-IG	HP LaserJet Managed MFP E62655, E62665, HP LaserJet Managed Flow MFP E62665, E62675 Installation Guide, HP Inc., 04/2019, Edition 1
E67650_60-UG	HP Color LaserJet Managed MFP E67650, HP Color LaserJet Managed Flow MFP E67660 User Guide, HP Inc., 04/2019, Edition 1
E67650_60-IG	HP Color LaserJet Managed MFP E67650, E67660 Installation Guide, HP Inc., 04/2019, Edition 1
M528-UG	HP LaserJet Enterprise MFP M528 HP LaserJet Enterprise Flow MFP M528 User Guide, HP Inc., 04/2019, Edition 1
M528-IG	HP LaserJet Enterprise MFP M528 Install Guide, HP Inc., 04/2019, Edition 1
E52645-UG	HP LaserJet Managed MFP E52645 HP LaserJet Managed Flow MFP E52645 User Guide, HP Inc., 04/2019, Edition 1
E52645-IG	HP LaserJet Enterprise MFP E52645 Install Guide, HP Inc., 04/2019, Edition 1

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.23.2	2020-05-11	None
1.23.1	2020-03-06	None
1.23	2019-10-14	Cryptographic implementation in environment now only allowed for EAL4 and above. This certification received an exemption as the application was accepted before this policy was in effect.
1.22.3	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL2:
SN-18	2.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	2.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-28	1.0	Updated procedures application, evaluation and certification	Evaluator reports should be received in two batches.