CSEC

Swedish Certification Body for IT Security

Certification Report - HP GIF

Issue: 1.0, 2019-Oct-11

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is the FutureSmart 4.5.1 firmware for the model series
HP LaserJet Managed MFP E72525 / E72530 / E72535,
HP Color LaserJet Managed MFP E77822 / E77825 / E77830,
HP LaserJet Managed MFP E82540 / E82550 / E82560,
HP Color LaserJet Managed MFP E87640 / E87650 / E87660,
HP LaserJet Enterprise MFP M631 / M632 / M633,
HP LaserJet Managed MFP E62555 / E62565 / E62575,
HP Color LaserJet Enterprise MFP M681 / M682, and
HP Color LaserJet Managed MFP E67550 / E67560.

These MFPs provide functions for network printing, copying, faxing, scanning, storing, and retreiving of documents.

The evaluated security features include intrusion detection, administrator and user identification and authentication, encrypted network communication (IPSec), encrypted storage of files, access control, audit etc.

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, 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 26th of August 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 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 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 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 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	CSEC2017009
Name and version of the certified IT product	FutureSmart 4.5.1 firmware for the MFP model series listed below
Security Target	HP LaserJet Managed MFP E72525 / E72530 / E72535, HP Color LaserJet Managed MFP E77822 / E77825 / E77830, HP LaserJet Managed E82540 / E82550 / E82560, HP Color LaserJet Managed MFP E87640 / E87650 / E87660, HP LaserJet Enterprise MFP M631 / M632 / M633, HP LaserJet Managed MFP E62555 / E62565 / E62575, HP Color LaserJet Enterprise MFP M681 / M682, HP Color LaserJet Managed MFP E67550 / E67560 Security Target
Assurance packages	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	1.22.3
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2019-10-11

Certified product versions (system firmware, JetDirect firmware, model series):

2405268_022691 JSI24050246 HP Color LaserJet Enterprise MFP M681

2405268_022691 JSI24050246 HP Color LaserJet Enterprise MFP M682

2405268_022691 JSI24050246 HP Color LaserJet Managed MFP E67550

2405268_022691 JSI24050246 HP Color LaserJet Managed MFP E67560

2405268_022692 JSI24050246 HP Color LaserJet Managed MFP E87640

2405268_022692 JSI24050246 HP Color LaserJet Managed MFP E87650

2405268_022692 JSI24050246 HP Color LaserJet Managed MFP E87660

2405268_022693 JSI24050246 HP LaserJet Managed MFP E82540

2405268_022693 JSI24050246 HP LaserJet Managed MFP E82550

2405268_022693 JSI24050246 HP LaserJet Managed MFP E82560

2405268_022694 JSI24050246 HP Color LaserJet Managed MFP E77822

2405268_022694 JSI24050246 HP Color LaserJet Managed MFP E77825

2405268_022694 JSI24050246 HP Color LaserJet Managed MFP E77830

2405268_022695 JSI24050246 HP LaserJet Managed MFP E72525

2405268_022695 JSI24050246 HP LaserJet Managed MFP E72530

2405268_022695 JSI24050246 HP LaserJet Managed MFP E72535

2405268_022699 JSI24050246 HP LaserJet Enterprise MFP M631

2405268_022699 JSI24050246 HP LaserJet Enterprise MFP M632

2405268_022699 JSI24050246 HP LaserJet Enterprise MFP M633

2405268_022699 JSI24050246 HP LaserJet Managed MFP E62555

2405268_022699 JSI24050246 HP LaserJet Managed MFP E62565

2405268_022699 JSI24050246 HP LaserJet Managed MFP E62575

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptography
- Identification and Authentication
- Protection of the TSF
- TOE Access Protection
- Trusted Channel communication and Certificate Management
- Security 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 security relevant functions. Both the Jetdirect Inside Firmware and System Firmware generate audit records. The TOE connects and sends audit records to an external syslog server for long-term storage and audit review.

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec.

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 cetificates 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, TOE can optionally 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 Security 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.

A.ADMIN.TRUST

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

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.

A.SERVICES.RELIABLE

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

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, administrators 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.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.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.REMOTE_PANEL.DISALLOWED

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

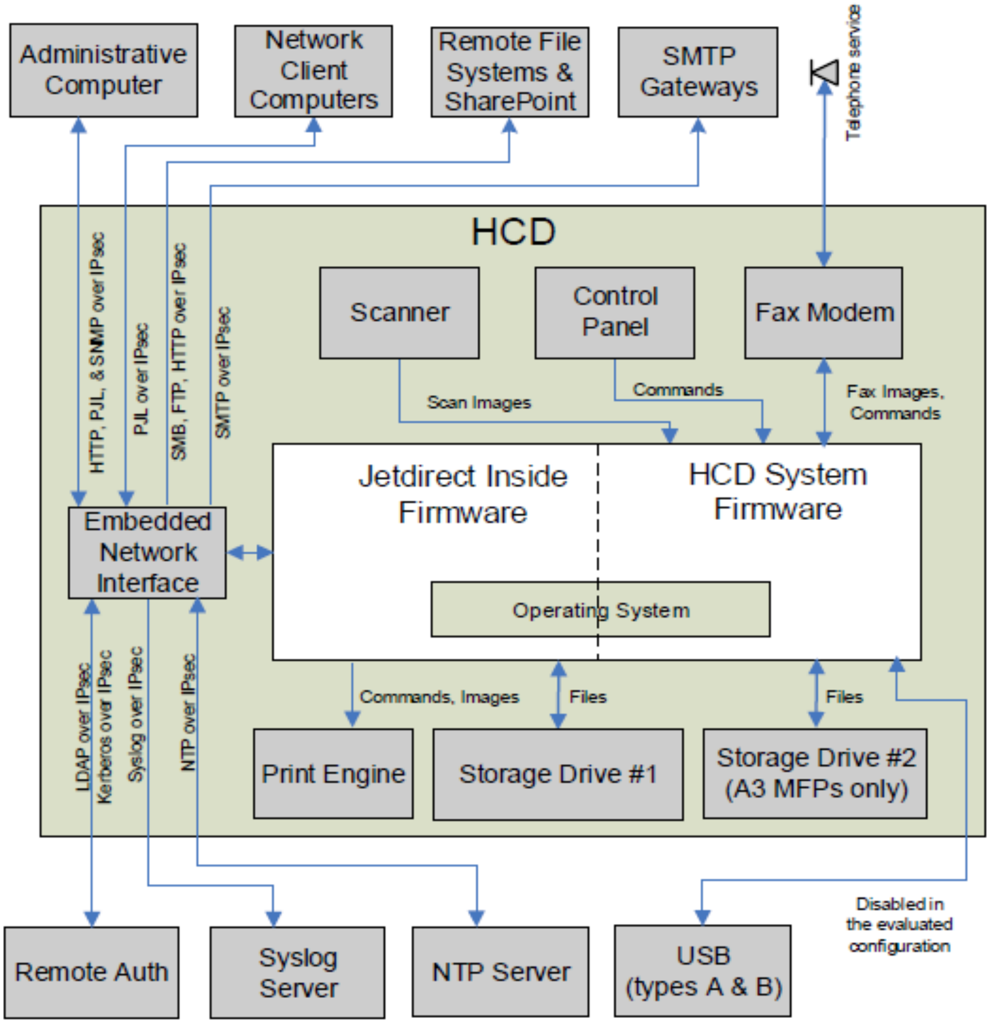
P.USERNAME.CHARACTER_SET

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).

5 Architectural Information

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 descripions 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 M631/M632/M633, HP Color LaserJet Enterprise MFP M681/M682, HP LaserJet Managed MFP E72525/E72530/E72535/E82540/E82550/E82560/E62555/E62565/E62575, HP Color LaserJet Managed MFP E77822/E77825/E77830/E87640/E87650/E87660/E67550/E67560
E825_E876	HP LaserJet Managed MFP E82540, HP LaserJet Managed MFP E82550, HP LaserJet Managed MFP E82560, HP LaserJet Managed Flow MFP E82540, HP LaserJet Managed Flow MFP E82550, HP LaserJet Managed Flow MFP E82560, HP Color LaserJet Managed MFP E87640, HP Color LaserJet Managed MFP E87650, HP Color LaserJet Managed MFP E87660, HP Color LaserJet Managed Flow MFP E87640, HP Color LaserJet Managed Flow MFP E87650, HP Color LaserJet Managed Flow MFP E87660 User Guide
E725_E778	HP LaserJet Managed MFP E72525, HP LaserJet Managed MFP E72530, HP LaserJet Managed MFP E72535, HP LaserJet Managed Flow MFP E72525, HP LaserJet Managed Flow MFP E72530, HP LaserJet Managed Flow MFP E72535, HP Color LaserJet Managed MFP E77822, HP Color LaserJet Managed MFP E77825, HP Color LaserJet Managed MFP E77830, HP Color LaserJet Managed Flow MFP E77822, HP Color LaserJet Managed Flow MFP E77825, HP Color LaserJet Managed Flow MFP E77830 User Guide
M63x	HP LaserJet Enterprise MFP M631, M632, M633 User Guide
M68x	HP Color LaserJet Enterprise MFP M681, M682 M633 User Guide

7 IT Product Testing

7.1 Developer Testing

The developers tested the TOE on four hardware models, both automatically and manually. The developer tests cover all TSFI, all SFRs and all subsystems.

All test results were as expected.

The testing was performed in the developers premises in Boise, Idaho, USA.

7.2 Evaluator Testing

The evaluators tested the TOE on five hardware models. Among these, three models were tested manually, four models were tested automatically, and two models were tested with static IP addresses.

The evaluators re-ran a sample of manual developer tests as well as all automated tests, and some customisations of the automated tests.

All test results were as expected.

The evaluators automated testing was performed at the developer site in Boise, Idaho, USA. The manual and static IP testing was performed in the evaluators own pemises in Stockholm, Sweden.

All test results were as expected.

7.3 Penetration Testing

The evaluators penetration tested the TOE on three hardware models.

The evaluators examined all potential interfaces (UDP and TCP ports), for IP v4 and for IP v6. Also, the SNMP port (UDP 161) was fuzzed.

The testing was performed in the evaluators premises in Stockholm, Sweden.

The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec, which is the expected result. No SNMP anomalies were discovered.

8 Evaluated Configuration

The following items will 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
- 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
- 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
- External file system access through PJL and PS 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 must have zero permissions enabled (this disables the Guest role)
- SNMP support limited to:
  - SNMPv1 read-only
  - SNMPv2c read-only
  - SNMPv3
- 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 Direct Print 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 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
- Fax polling receive must be disabled
- User Access Codes use is disabled
- An IPv4 address must be statically assigned as per the instructions in TOE's configuration guidance [CCECG]

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
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_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Flaw Remediation	ALC_FLR.2	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
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 LaserJet Managed MFP E72525 / E72530 / E72535, HP Color LaserJet Managed MFP E77822 / E77825 / E77830, HP LaserJet Managed E82540 / E82550 / E82560, HP Color LaserJet Managed MFP E87640 / E87650 / E87660, HP LaserJet Enterprise MFP M631 / M632 / M633, HP LaserJet Managed MFP E62555 / E62565 / E62575, HP Color LaserJet Enterprise MFP M681 / M682, HP Color LaserJet Managed MFP E67550 / E67560 Security Target, HP Inc., 2019-08-16, document version 2.62
CCECG	Common Criteria Evaluated Configuration Guide for HP Multifunction Printers HP LaserJet Enterprise MFP M631/M632/M633, HP Color LaserJet Enterprise MFP M681/M682, HP LaserJet Managed MFP E72525/E72530/E72535/E82540/E82550/E82560/E62555/E62565/E62575, HP Color LaserJet Managed MFP E77822/E77825/E77830/E87640/E87650/E87660/E67550/E67560, HP Inc., 2019-04, document version 1
PP2600A	2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, IEEE, June 2009, document version 1.0
E825_E876	HP LaserJet Managed MFP E82540, HP LaserJet Managed MFP E82550, HP LaserJet Managed MFP E82560, HP LaserJet Managed Flow MFP E82540, HP LaserJet Managed Flow MFP E82550, HP LaserJet Managed Flow MFP E82560, HP Color LaserJet Managed MFP E87640, HP Color LaserJet Managed MFP E87650, HP Color LaserJet Managed MFP E87660, HP Color LaserJet Managed Flow MFP E87640, HP Color LaserJet Managed Flow MFP E87650, HP Color LaserJet Managed Flow MFP E87660 User Guide, HP Inc., 2018-04, Edition 2
E725_E778	HP LaserJet Managed MFP E72525, HP LaserJet Managed MFP E72530, HP LaserJet Managed MFP E72535, HP LaserJet Managed Flow MFP E72525, HP LaserJet Managed Flow MFP E72530, HP LaserJet Managed Flow MFP E72535, HP Color LaserJet Managed

MFP E77822, HP Color LaserJet Managed MFP E77825, HP Color LaserJet Managed MFP E77830, HP Color LaserJet Managed Flow MFP E77822, HP Color LaserJet Managed Flow MFP E77825, HP Color LaserJet Managed Flow MFP E77830 User Guide, HP Inc., 2018-04, Edition 2

M63x HP LaserJet Enterprise MFP M631, M632, M633 User Guide, HP Inc., 2017-10, Edition 3

M68x HP Color LaserJet Enterprise MFP M681, M682 M633 User Guide, HP Inc., 2017-05, Edition 1

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 2017-06-16:

QMS 1.20.4	valid from 2017-05-11
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
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 1.20.4 to the current QMS 1.22.3, there are no changes with impact on the result of the certification.