Swedish Certification Body for IT Security

Certification Report - HP Intrusion Detection

Issue: 1.0, 2019-maj-24

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

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

HP LaserJet Enterprise MFP M630 Series

HP LaserJet Enterprise 500 MFP M525 Series

HP Color LaserJet Enterprise Printer M651 Series

HP LaserJet Enterprise 500 color MFP M575 Series

HP Officejet Enterprise Color MFP X585 Series

HP Officejet Enterprise Color Printer X555 Series

HP Color LaserJet Enterprise Printer M855 Series

HP Color LaserJet Enterprise MFP M680 Series

HP Color LaserJet Enterprise flow MFP M880 Series

HP LaserJet Enterprise MFP M725 Series

HP LaserJet Enterprise flow MFP M830 Series

HP Color LaserJet Enterprise MFP M577 Series

HP LaserJet Enterprise MFP M527 Series

HP PageWide Enterprise Color Printer 556 Series

HP PageWide Enterprise Color MFP 586 Series

HP LaserJet Enterprise Printer M506 Series

HP LaserJet Enterprise Printer M605 Series

HP LaserJet Enterprise Printer M606 Series

HP Color LaserJet Enterprise Printer M553 Series

These SFPs and MFPs provide network printing and storing, depending on model also faxing and scanning.

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

The library in QuickSec that provides cryptographic support for IPSec is considered part of the operational environment but the cryptographical functions used by the TOE has been tested as part of the evaluation.

The ST does not claims conformance to any Protection Profile.

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 6th of May 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 2, augmented by ALC_FLR.2.

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 2 + 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.

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. The effect of invoking the cryptographic primitives used by the TOE have been tested within the scope of the evaluation.

2 Identification

Certification Identification	
Certification ID	CSEC2016006
Name and version of the certified IT product	HP Enterprise LaserJet, Officejet, and PageWide single-function printer (SFP) and multifunction printer (MFP) FutureSmart firmware (models listed below)
Security Target	Intrusion Detection in the HP Enterprise LaserJet, Officejet, and PageWide SFP and MFP FutureSmart Firmware Security Target
Assurance packages	EAL 2 + 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	1.22.2
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2019-05-24

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

2405268_022701 JDI24050229 HP LaserJet Enterprise MFP M630 Series
2405268_022702 JDI24050229 HP LaserJet Enterprise 500 MFP M525 Series
2405268_022703 JDI24050229 HP Color LaserJet Enterprise Printer M651 Series
2405268_022704 JDI24050229 HP LaserJet Enterprise 500 color MFP M575 Series
2405268_022705 JDI24050229 HP Officejet Enterprise Color MFP X585 Series
2405268_022721 JDI24050229 HP Officejet Enterprise Color Printer X555 Series
2405268_022724 JDI24050229 HP Color LaserJet Enterprise Printer M855 Series
2405268_022738 JDI24050229 HP Color LaserJet Enterprise MFP M680 Series
2405268_022739 JDI24050229 HP Color LaserJet Enterprise flow MFP M880 Series
2405268_022740 JDI24050229 HP LaserJet Enterprise MFP M725 Series
2405268_022741 JDI24050229 HP LaserJet Enterprise flow MFP M830 Series
2405268_022696 JSI24050246 HP Color LaserJet Enterprise MFP M577 Series
2405268_022698 JSI24050246 HP LaserJet Enterprise MFP M527 Series

2405268_022711 JSI24050246 HP PageWide Enterprise Color Printer 556 Series
2405268_022716 JSI24050246 HP PageWide Enterprise Color MFP 586 Series
2405268_022717 JSI24050246 HP LaserJet Enterprise Printer M506 Series
2405268_022718 JSI24050246 HP LaserJet Enterprise Printer M605 Series
2405268_022718 JSI24050246 HP LaserJet Enterprise Printer M606 Series
2405268_022726 JSI24050246 HP Color LaserJet Enterprise Printer M553 Series

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.

For intrusion detection, the TOE uses the Message Digest 5 (MD5) algorithm to perform integrity checks on the XIP (execute in-place) code.

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. When a user signs in through the Control Panel, the TOE displays either asterisks or dots (depending on the HCD model) for each character entered of the Administrator Access Code and remote sign-in password to prevent onlookers from viewing another user's authentication data.

The Control Panel uses permissions to determine which control panel applications a user can access. The built-in Device Administrator account has the Device Administrator Permission Set permanently assigned to it. For a user that signs in via LDAP or Kerberos, the user's session permission set may include the network user account's permission set, a permission set based on the set of network groups for which the user is a member, or the remote sign-in method's permission set. A control panel user's role is determined by the session permission set.

The Control Panel implements two account lockout mechanisms. The first mechanism, upon detection of a pre-configured maximum failed attempts to log into the local Device Administrator account, locks the account before the lockout interval has elapsed. The other mechanism (called Simplified Account Lockout) is used for the other control panel account types. It inserts a 10 second delay between authentication attempts when 6 failed authentication attempts for a user account have been detected within a 5 minute period.

● 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.

The IPsec/Firewall service templates define the user role of a client computer. The All Services service template is used to define the Administrator Computer for IPsec users. The Administrative Computer can access the PJL Interface on port 9100 as well as the EWS (HTTP) interface, Web Services interface (OXPd and WS*), and SNMP interface.

3.4 Protection of the TSF

● Intrusion Detection

Once the TOE is instantiated, the TOE runs continuous, cryptographic integrity checks on XIP code. If the TOE detects an intrusion from the failure of one or more of these integrity checks, the TOE will attempt to perform the following notifications:

- Generate and forward an audit record to the syslog server
- Create an entry in the event log stored in the TOE
- Display an error message on the Control Panel

In addition, the TOE will attempt to perform the following actions:

- Take device offline
- Initiate a reboot of the TOE
- Upon restart of the system and depending on an administrator configurable auto-recovery option, either halt the boot process in the Basic Input/Output System (BIOS) awaiting human confirmation or continue into a full reboot of the TOE

Depending on the extent of the intrusion, the TOE may or may not be able to perform one or more of these notifications and actions.

● Reliable Timestamps

The TOE contains a system clock that is used to generate reliable timestamps. Only an administrator can manage the system clock.

3.5 TOE Access Protection

● Inactivity Timeout

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. The inactivity period is managed by the administrator via EWS (HTTP), WS* web services, or the Control Panel. A single inactivity period setting exists per TOE.

3.6 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.

3.7 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.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes six 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.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 sent by the TOE to the SMTP gateway, the transmission of emails from the SMTP gateway to the email's destination is protected.

A.SERVICES.RELIABLE

When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, 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 five threats, which have been considered during the evaluation.

T.TSF_DATA.IN_TOE_DIS

TSF data in the TOE may be disclosed by unauthorized persons.

T.TSF_DATA.IN_TOE_MOD

TSF data in the TOE may be modified by unauthorized persons.

T.TSF_DATA.IN_TRANSIT_DIS

TSF data on the network may be disclosed by unauthorized persons.

T.TSF_DATA.IN_TRANSIT_MOD

TSF data on the network may be modified by unauthorized persons.

T.XIP.MOD

The TOE's XIP code may be modified (corruption or injection of malware) by unauthorized persons.

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

P.ADMIN.AUTHORIZATION

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

P.ADMIN.PASSWORD

To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that this password is required to perform security-relevant actions through EWS (HTTP), OXPd, WS* Web Services, or 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 by the TOE. Exported audit records will be protected from unauthorized disclosure or modification 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 Operational Environment.

P.REMOTE_PANEL.DISALLOWED

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

P.RSA.KEYSIZE

To preserve IPsec communications security, all devices connecting to the TOE via IPsec must be configured to use an RSA key size of 2048-bits or greater.

P.USERNAME.CHARACTER_SET

To prevent ambiguous user names in the TOE's audit trail, the Display Names of the Local Device Sign In method users and the user names of the LDAP and Windows Sign In method 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

The TOE firmware contains intrusion detection functionality designed to detect modifications to execute in-place (XIP) code. XIP code is defined as the code in the kernel that is built to execute from a specific location in memory, and this location cannot be changed at runtime. When the TOE is initially loaded, it verifies the signatures of the loaded components to ensure that the TOE has not been modified. Once loaded, the intrusion detection code continuously scans the XIP code looking for modifications. Upon detecting a modification, the TOE attempts to perform the following notifications:

● Generate and forward an audit record to the syslog server

● Create an entry in the event log stored in the TOE

● Display an error message on the Control Panel In addition, the TOE will attempt to perform the following actions:

● Take device offline

● Initiate a reboot of the TOE

● Upon restart of the system and depending on an administrator configurable auto-recovery option, either halt the boot process in the BIOS awaiting human confirmation or continue into a full reboot of the TOE

The intrusion detection functionality, along with the printing, copying, scanning, faxing, and storing of documents, is a standard part of the HCD firmware.

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

The Web Services allows an administrator to remotely manage the TOE over the network. The TOE supports both HP's OXPd Web Services and certain WS* Web Services (conforming to the WS* standards defined by w3.org) accessed via the SOAP and XML. These interfaces are also protected using IPsec.

The SNMP network interface allows an administrator to remotely manage the TOE using external SNMP-based administrative applications. The evaluated configuration supports SNMPv1 read only, SNMPv2c read only and SNMPv3. This interface is protected using IPsec.

Printer Job Language (PJL) is 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 IPsec. Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using X.509v3 certificates. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) into the TOE along 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 other 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.

The TOE also supports Microsoft SharePoint (flow MFP models only) and remote file systems for the storing of scanned documents. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to SharePoint and the remote file systems. For remote file system connectivity, the TOE supports the FTP and SMB protocols.

Some HCD models containing the TOE can be used to email scanned documents, email received faxes, or email sent faxes. The TOE can send email alert messages to administrator-specified email addresses, or send automated emails regarding product configuration and MFP supplies to HP. The TOE supports protected communications between itself and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate with the SMTP gateway. The TOE can only protect unencrypted emails 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.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of either a touchscreen LCD or a 4-line display (depending on the HCD model), a physical power button, and a physical home screen button that are attached to the HCD. In addition, flow MFP models include 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 touchscreen LCD 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. The 4-line display displays status to the user.

6 Documentation

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

CCECG	HP Common Criteria Evaluated Configuration Guide for HP Enterprise LaserJet, Officejet, and PageWide Single-Function and Multifunction Printers running HP FutureSmart Firmware with Intrusion
UGPW556	HP PageWide Enterprise Color 556 User Guide
UGPW586	HP PageWide Enterprise Color MFP 586 User Guide
UGM506	HP LaserJet Enterprise M506 User Guide
UGM525	HP LaserJet Enterprise 500 MFP M525 User Guide
UGM525	HP LaserJet Enterprise Flow MFP M525 User Guide
UGM527	HP LaserJet Enterprise MFP M527 User Guide
UGM552/3	HP Color LaserJet Enterprise M552/M553 User Guide
UGM575	HP LaserJet Enterprise 500 Color MFP M575 User Guide
UGM575	HP LaserJet Enterprise Color Flow MFP M575 User Guide
UGM577	HP Color LaserJet Enterprise MFP M577 User Guide
UGM604/5/6	HP LaserJet Enterprise M604, M605, M606 User Guide
UGM630	HP LaserJet Enterprise MFP M630 User Guide
UGM651	HP Color LaserJet Enterprise M651 User Guide
UGM680	HP Color LaserJet Enterprise MFP M680 User Guide
UGM725	HP LaserJet Enterprise MFP M725 User Guide
UGM830	HP LaserJet Enterprise Flow MFP M830 User Guide
UGM855	HP Color LaserJet Enterprise M855 User Guide
UGM880	HP Color LaserJet Enterprise Flow MFP M880 User Guide
UGX555	HP Officejet Enterprise Color X555 User Guide
UGX585	HP Officejet Enterprise Color MFP X585/Flow X585 User Guide

7 IT Product Testing

7.1 Developer Testing

The developers tested all TSFI both automatically and manually. All product model series were tested manually, and all but one were tested automatically. All test results were as expected.

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

7.2 Evaluator Testing

Four TOE models were used for evaluator testing. The evaluators re-run a sample of manual developer tests as well as all automated tests, and some customisations of the automated tests. A developer tool were used to verify that the intrusion detection were effective against memory alterations.

The evaluators performed the automated and manual testing on 11 to 21 of September 2018 at the developer site in Boise, Idaho, USA.

All test results were as expected.

7.3 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, which is the expected result.

8 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.
- HP and third-party applications cannot be installed on the TOE.
- All received faxes must be stored in Job Storage.
- Fax Forwarding and Fax Archiving must be disabled.
- PC Fax Send must be disabled.
- Device USB and Host USB plug and play must be disabled.
- FIH port must be disabled.
- Remote Firmware Upgrade through any means other than 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.
- External file system access through PJL and PostScrit (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.
- Full Authentication must be enabled (this disables the Guest role).
- SNMP support is 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.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- The "Save to HTTP" function is disallowed and must not be configured to function with an HTTP server.
- Display Names for the Local Device Sign In method users and user names for the LDAP and Windows Sign In method users must only contain the characters defined in P.USERNAME.CHARACTER_SET.
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.DISALLOWED.
- User Access Codes use is disallowed.

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
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	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.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.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.1	PASS
Functional Tests	ATE_FUN.1	PASS

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

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 — Intrusion Detection in the HP Enterprise LaserJet, Officejet, and PageWide SFP and MFP FutureSmart Firmware Security Target, HP Inc., 2019-04-15, document version 2.3

CCECG — HP Common Criteria Evaluated Configuration Guide for HP Enterprise LaserJet, Officejet, and PageWide Single-Function and Multifunction Printers running HP FutureSmart Firmware with Intrusion Detection, HP Inc., 2019-03-07, document version 1.7

UGPW556 — HP PageWide Enterprise Color 556 User Guide, HP Inc., 2016-05, Edition 1

UGPW586 — HP PageWide Enterprise Color MFP 586 User Guide, HP Inc., 2016-05, Edition 1

UGM506 — HP LaserJet Enterprise M506 User Guide, HP Inc., 2017-08, Edition 2

UGM525 — HP LaserJet Enterprise 500 MFP M525 User Guide, HP Inc., 2017-08, Edition 1

UGM525f — HP LaserJet Enterprise Flow MFP M525 User Guide, HP Inc., 2017-08, Edition 1

UGM527 — HP LaserJet Enterprise MFP M527 User Guide, HP Inc., 2015-08, Edition 2

UGM552/3 — HP Color LaserJet Enterprise M552/M553 User Guide, HP Inc., 2015-11, Edition 1

UGM575 — HP LaserJet Enterprise 500 Color MFP M575 User Guide, HP Inc., 2012-05, Edition 1

UGM575f — HP LaserJet Enterprise Color Flow MFP M575 User Guide, HP Inc., 2012-11, Edition 2

UGM577 HP Color LaserJet Enterprise MFP M577 User Guide, HP Inc., 2015-11, Edition 1

UGM604/5/6 HP LaserJet Enterprise M604, M605, M606 User Guide, HP Inc., 2017-08, Edition 2

UGM630 HP LaserJet Enterprise MFP M630 User Guide, HP Inc., 2017-08, Edition 2

UGM651 HP Color LaserJet Enterprise M651 User Guide, HP Inc., 2015-11, Edition 1

UGM680 HP Color LaserJet Enterprise MFP M680 User Guide, HP Inc., 2015-11, Edition 1

UGM725 HP LaserJet Enterprise MFP M725 User Guide, HP Inc., 2017-08, Edition 2

UGM830 HP LaserJet Enterprise Flow MFP M830 User Guide, HP Inc., 2017-08, Edition 2

UGM855 HP Color LaserJet Enterprise M855 User Guide, HP Inc., 2015-11, Edition 1

UGM880 HP Color LaserJet Enterprise Flow MFP M880 User Guide, HP Inc., 2015-11, Edition 1

UGX555 HP Officejet Enterprise Color X555 User Guide, HP Inc., 2014-04, Edition 1

UGX585 HP Officejet Enterprise Color MFP X585/Flow X585 User Guide, HP Inc., 2015-11, 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 2016-06-17:

QMS 1.19.3	valid from 2016-06-02
QMS 1.20	valid from 2016-10-20
QMS 1.20.1	valid from 2017-01-12
QMS 1.20.2	valid from 2017-07-27
QMS 1.20.3	valid from 2017-04-24
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

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 1.22.2".

The certifier concluded that, from QMS 1.19.3 to the current QMS 1.22.2, there are no changes with impact on the result of the certification.