Swedish Certification Body for IT Security

Certification Report HP MEYVA

Issue: 1.0, 2015-okt-06

Authorisation: Jerry Johansson, , CSEC

Table of Contents

1   Executive Summary

The Target of Evaluation, TOE, is the firmware of a network printer, with the exception of the operating system and the crypto module implementation. Five versions of the printer are included in the scope of the evaluation: the LaserJet Enterprise M506 Printer Series, the LaserJet Enterprise M604 Printer Series, the LaserJet Enterprise M605 Printer Series, the LaserJet Enterprise M606 Printer Series (black and white), and the Color LaserJet Enterprise M553 Printer Series (color).

These printers provide network printing functionality, and print jobs can be stored and printed from the console. The network connections are encrypted, password protected print jobs are encrypted, PIN protected print jobs are protected by access control, and stored jobs may be printed from the printer console.

The evaluated security features include administrator and user identification and authentication, PIN or password protected encryption of jobs, and IPSec protected network communication.

The implementation of the cryptographic module used for IPSec is outside the scope of the evaluation, but the effect of cryptographic function calls from the TOE has been verified. Other cryptographic implementations are within the scope of TOE.

The USB interface is disabled in the evaluated configuration.

The ST claims conformance to:

2600.2 PP, Protection Profile for Hardcopy Devices, Operational Environment B; Version 1.0; March 2009, in accordance with the NIAP CCEVS Policy Letter #20. The claim includes the following packages from the PP:

2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B

2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B

2600.2-SMI, SFR Package for Hardcopy Device Shared-Medium Interface Functions, Operational Environment B

The evaluation has verified demonstrable conformance to the PP and conformance to the package claims stated above.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, and to some extent in the approved foreign location in Austin, Texas, USA, and was completed on the 4th of September 2015.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 2, augmented by ALC_FLR.2 Flaw reporting procedures.

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 evaluation assurance level:

EAL 2 + ALC_FLR.2.

2   Identification

Certification Identification

Certification ID	CSEC2015002

Name and version of the
certified IT product and
the TOE

HP LaserJet Enterprise M506 Printer Series
(M506n, M506dn, and M506x)
> MFP firmware version 2305076_518482
> JetDirect firmware version JSI23500060

HP LaserJet Enterprise M604 Printer Series
(M604n, and M604dn)
> MFP firmware version 2305076_518485
> JetDirect firmware version JSI23500060

HP LaserJet Enterprise M605 Printer Series
(M605n, M605dn, M605dh, and M605x)
> MFP firmware version 2305076_518485
> JetDirect firmware version JSI23500060

HP LaserJet Enterprise M606 Printer Series
(M606dn, and M606x)
> MFP firmware version 2305076_518485
> JetDirect firmware version JSI23500060

HP Color LaserJet Enterprise M553 Printer Series
(M553n, M553dn, M553dh, and M553x)
> MFP firmware version 2305076_518484
> JetDirect firmware version JSI23500060

Security Target

HP LaserJet Enterprise M506 Printer
Series, Color LaserJet Enterprise M553 Printer Series,
LaserJet Enterprise M604 Printer Series, LaserJet
Enterprise M605 Printer Series, and LaserJet
Enterprise M606 Printer Series Firmware with
Jetdirect Inside Security Target
HP Inc. 2015-09-28, document version 2.0

Assurance level	EAL 2 + ALC_FLR.2
Sponsor	HP Inc.
Developer	HP Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2015-10-06

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

3.1 Auditing

The TOE generates audit records for security relevant events. The audit records are sent to a syslog server in the environment for storage and audit review.

3.2 Cryptography

The external communication channels are protected with IPSec (the IPSec implementation is part of the operational environment), and print jobs can be encrypted based on a password (the implementation of print job decryption is part of the TOE).

3.3 Identification and Authentication

Console access requires user identification and authentication.

3.4 Data Protection and Access Control

Stored jobs are protected by PIN (access control) or password (encryption). In addition, the access to read, modify and delete operations are controlled based on user identity and job ownership.

3.5 Protection of the TSF

Restricted forwarding - the TOE does not allow forwarding of data to external interfaces.

There are integrity tests, which the administrators can execute, to verify TSF data and code.

The TOE contains a system clock which provides reliable time stamps. In the evaluated configuration, the TOE system clock will synchronise with an NTP server.

3.6 TOE Access Protection

Control panel access is protected by an inactivity timeout, which will terminate sessions after a certain time, configurable by the administrators.

3.7 Trusted Channel Communication and Certificate Management

All network access to the TOE requires the use of an integrity and confidentiality protected trusted channel.

TOE provides a mechanism to import X.509 v3 certificates.

3.8   User and Access Management

Only administrators have authority to manage security functionality, users, and the external authenticated servers.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.USER.TRAINING - TOE users are aware of the security policies and the 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.

4.2 Environmental Assumptions

Four assumptions on the environment are made in the Security Target.

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

4.3 Clarification of Scope

The Security Target [ST] 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 by unauthorized persons.

T.CONF.ALT - TSF Confidential Data may be altered by unauthorized persons.

5 Architectural Information

The TOE is the firmware of an enterprise network printer designed to be shared by many client computers and human users. It performs the functions of storing and printing printjobs. It can be connected to a local network through the embedded Jetdirect Inside print server's built-in Ethernet.
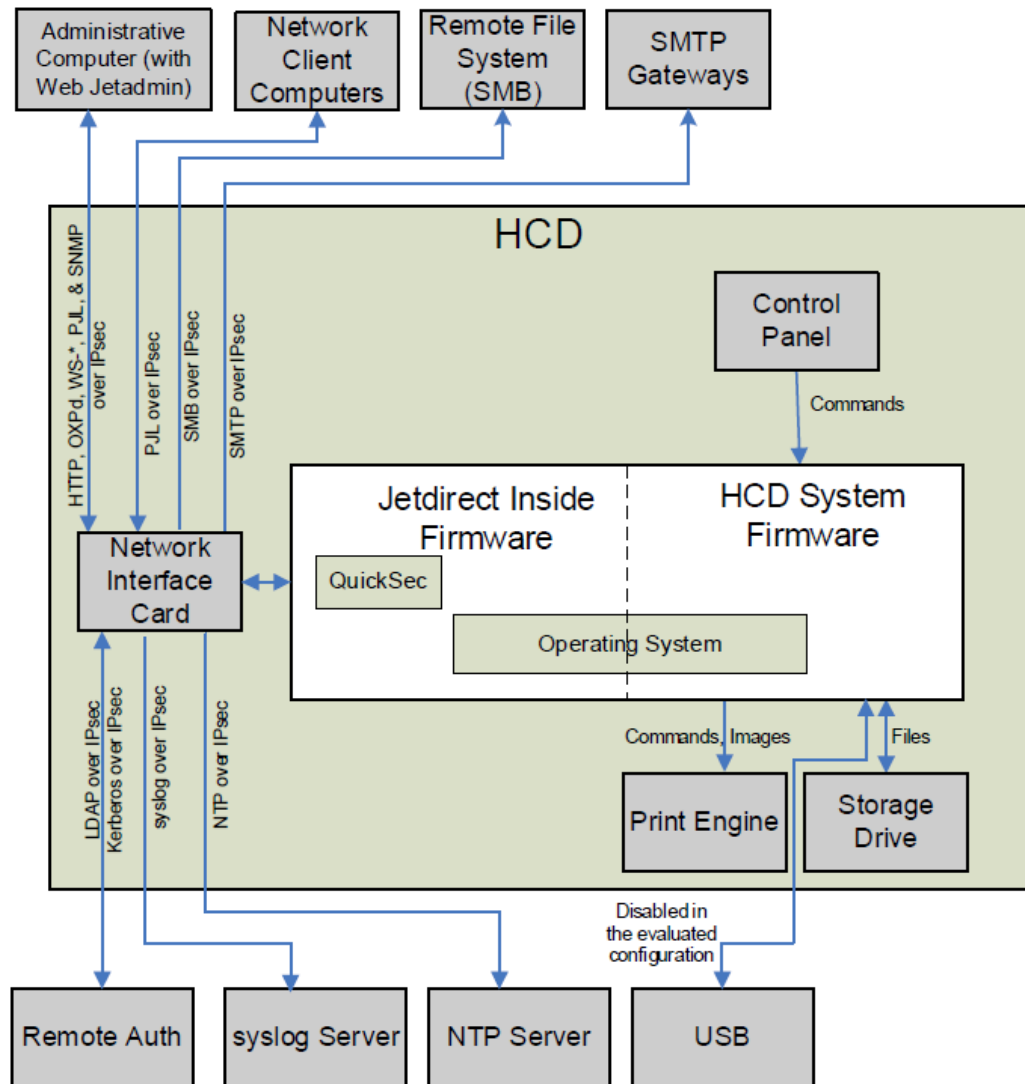
Figure 1: HCD physical diagram

Figure 1 shows a high-level physical diagram of a Hardcopy Device (HCD) with the unshaded areas representing the TOE and the shaded areas indicating components that are part of the Operational Environment.

At the top of this figure is the Administrative Computer which connects to the TOE using Internet Protocol Security (IPsec) with X.509v3 certificates for both mutual authentication and for protection of data from disclosure and alteration. This computer can administer the TOE using the following interfaces over the IPsec connection:

● Embedded Web Server (EWS)

● Simple Network Management Protocol (SNMP)

- Web Services:
  - Open Extensibility Platform device (OXPd) Web Services
  - WS-* Web Services

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

The Web Services allow administrators to manage the TOE using HP's Web Jetadmin application, which is part of the Operational Environment. The TOE supports both HP's Open Extensibility Platform device (OXPd) Web Services and certain WS-* Web Services (conforming to the WS-*standards defined by w3.org) accessed via the Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML).

The SNMP network interface allows administrators to remotely manage the TOE using external SNMP-based administrative applications like the HP Web Jetadmin administrative tool.

Printer Job Language (PJL) is used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL 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. For the purposes of the evaluation, we define the PJL Interface as PJL data sent to port 9100.

Web Jetadmin uses the HTTP, OXPd, PJL, SOAP/XML, WS-*, and SNMP protocols to manage the TOE. Remote applications such as web browsers and Web Jetadmin are part of the Operational Environment, not part of the TOE.

The TOE protects all network communications with Internet Protocol Security (IPsec), which is part of the embedded Jetdirect Inside firmware. 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 with the Certificate Authority's CA certificate.

Because IPsec authenticates the computers (IPsec authenticates the computer itself; IPsec does not authenticate 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.

The TOE can also communicate with trusted IT products using IPsec.

The evaluated configuration supports the following SNMP versions:

- SNMPv1 read-only
- SNMPv2c read-only
- SNMPv3

Network Client Computers connect to the TOE using IPsec with X.509v3 certificates to protect the communication and to mutually authenticate. These client computers can send print jobs to the TOE using the PJL Interface as well as receive job status.

The TOE protects stored jobs with either a 4-digit Job PIN or by accepting (and storing) a password encrypted job from a user computer. Both protection mechanisms are optional by default and are mutually exclusive of each other if used. In the evaluated configuration, every job must either be assigned a 4-digit Job PIN or be an encrypted job.

The TOE supports the Server Message Block (SMB) protocol. SMB is used by administrators to backup and restore customer-specific configuration settings and TSF data (local user account data). (It does not backup job files.) Only administrators can access the SMB through the TOE. The connection is protected using IPsec.

The TOE can send email alert messages to administrator-specified e-mail addresses. In addition, the TOE's AutoSend feature can send automated emails regarding product configuration and printer supplies to HP. The TOE supports protected communications between the TOE 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 email up to the SMTP gateway. It is the responsibility of the Operational

Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

Each HCD contains a user interface called the Control Panel. The Control Panel is the physical interface that a user uses to communicate with the TOE when physically using the HCD. Model numbers that end with "n", "dn", or "dh" have a Control Panel with a 4-line LCD non-touchscreen display. Model numbers that end with "x" have a Control Panel with a 4.3-inch LCD touchscreen display. Each Control Panel has an "Easy Access" USB port which is disabled in the evaluated configuration. Each Control Panel also has a set of physical buttons whose quantities and functions vary between models. Users use the Control Panel to sign in to the TOE and perform functions such as accessing and printing stored print jobs. When a user signs in at the Control Panel, a Permission Set is associated with that user's session which determines the functions the user is permitted to perform.

The TOE's Control Panel supports both local and remote sign in methods. The local sign in method is called Local Device Sign In which supports individual user accounts. The user account information is maintained in the Local Device Sign In database within the TOE. The remote sign in methods are called LDAP Sign In and Windows Sign In (Kerberos). The TOE uses IPsec with X.509v3 certificates to protect both the LDAP and Kerberos communications.

The Print Engine in Figure 1 converts electronic format into hardcopy.

All printer models contain a nonvolatile mass storage device (a.k.a. storage drive) that resides in the Operational Environment. The storage drive contains a section called Job Storage which is a user-visible file system where stored print jobs are stored/held. Depending on the printer model number, the storage drive is either an:

• Embedded MultiMediaCard (eMMC), or

• HP High Performance Secure Hard Disk

If the printer model contains an eMMC, all jobs in Job Storage are automatically deleted when the HCD is power-cycled. If the printer model contains an HP High Performance Secure Hard Disk, the jobs can persist across power-cycles or can be deleted, depending on how the administrator configures the TOE and on the job type.

The TOE supports the auditing of security relevant functions by generating and forwarding audit records to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between the TOE and the syslog server and to mutually authenticate the TOE and the syslog server.

The Jetdirect Inside Firmware and HCD System Firmware components comprise the firmware on the system. They are shown as two separate components but they both share the same operating system (OS). The operating system is part of the Operational Environment. Both firmware components also contain an Embedded Web Server (EWS).

The Jetdirect Inside firmware includes SNMP, IPsec, a firewall, and the management functions for managing these network-related features. The Jetdirect Inside firmware also provides the network stack and drivers controlling the TOE's Ethernet interface.

The HCD System Firmware controls the overall functions of the TOE from the Control Panel to the storage drive to the print jobs.

Figure 1 shows the HCD boundary in green and the firmware (TOE) boundary in white (the TOE being comprised of the HCD System firmware and the Jetdirect Inside firmware excluding the underlying operating system and the QuickSec cryptographic library). The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the HCD System firmware. The HCD System firmware and Jetdirect Inside firmware share the same operating system (which is part of the Operational Environment). The HCD System firmware also includes internal Control Panel applications that drive the functions of the TOE. Both firmware components work together to provide the security functionality defined in this document for the TOE.

6   Documentation

The following documents are included in the scope of the TOE:

LaserJet Enterprise M506 - User Guide

Color LaserJet Enterprise M553 - User Guide

LaserJet Enterprise M604, M605, M606 - User Guide

Common Criteria Evaluated Configuration Guide for HP Single-Function Printers

7 IT Product Testing

7.1 Developer Testing

The developer performed testing of the security functionality, as described by the security functional requirements in the Security Target, covering both IP v.4 and IP v.6, for all five hardcopy devices (M506, M553, M604, M605, and M606). The developer testing was performed in the developer's premises in Boise, Idaho, USA.

7.2 Evaluator Testing

Since the entire TSF is implemented in one firmware (JSI23500060), that is used by all TOE versions, the evaluators focused on two of the hardcopy devices (M553 and M605), which were tested in the atsec Evaluation Laboratory in Stockholm, Sweden.

The evaluators used the developer's test setup and verified a sample of the developer's test cases, covering all interfaces and security functions.

The evaluators also devised and performed additional test cases to provide full coverage of the security functions and TSFI.

7.3 Evaluator Penetration Testing

The evaluators performed variations of the functional tests to search for vulnerabilities in the TOE, and performed port scans of the network interface of the TOE, covering TCP and UDP ports both for IP v.4 and IP v.6. Penetration testing was performed on the hardcopy devices M553 and M605, in the atsec Evaluation Laboratory in Stockholm, Sweden.

8   Evaluated Configuration

The TOE shall run on either the M506, M553, M604, M605, or the M606 hardcopy device, and shall be configured in accordance with the CC Configuration Guide [CCcfg].

The following requirements applies to the evaluated configuration:

● 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 print jobs must be assigned a Job PIN or encrypted with a password

● Type A and B USB ports 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

● File System External 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 Authenticated Headers (AH) must be disabled

● Full Authentication must be enabled (this disables the Guest account)

● 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 Filed 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

● 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 as per P.REMOTE_PANEL.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 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 respective 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
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10   Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

AES	Advanced Encryption Standard
AH	Authentication Header (IPsec)
CBC	Cipher Block Chaining
CIFS	Common Internet File System
CRV	Constrained Random Verification
CTS	Cipher Text Stealing
DNS	Domain Name System
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
FTP	File Transfer Protocol
HCD	Hardcopy Device
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IKE	Internet Key Exchange (IPsec)
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NTP	Network Time Protocol
OXP	Open Extensibility Platform
OXPd	OXP device layer
PIN	Personal Identification Number
PJL	Printer Job Language
PML	Printer Management Language
PRF	Pseudo-random Function
PSTN	Public Switched Telephone Network
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TOE	Target of Evaluation
USB	Universal Serial Bus
WINS	Windows Internet Name Service
XML	Extensible Markup Language

12   Bibliography

ST	HP LaserJet Enterprise M506 Printer Series, Color LaserJet Enterprise M553 Printer Series, LaserJet Enterprise M604 Printer Series, LaserJet Enterprise M605 Printer Series, LaserJet Enterprise M606 Printer Series Firmware with Jetdirect Inside Security Target, HP Inc., 2015-09-28, document version 2.0
UG506	LaserJet Enterprise M506 - User Guide, Hewlett-Packard, 2015-10, Edition 1
UG553	Color LaserJet Enterprise M553 - User Guide, Hewlett-Packard, 2015-04, Edition 2
UG60*	LaserJet Enterprise M604, M605, M606 - User Guide, Hewlett-Packard, 2015-04, Edition 1
CCcfg	Common Criteria Evaluated Configuration Guide for HP Single-Function Printers, Hewlett-Packard, 2015-06, Edition 1
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 4, CCMB-2012-09-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 4, CCMB-2012-09-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 4, CCMB-2012-09-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2014-12-12, document version 22.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2013-06-18, document version 4.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2015-04-09:

QMS 1.17.3   valid from 2015-01-29

QMS 1.18   valid from 2015-06-18

QMS 1.18.1   valid from 2015-08-21

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 QMS 1.18.1".

The certifier concluded that, from QMS 1.17.3 to the current QMS 1.18.1, there are no changes with impact on the result of the certification.