CSEC

Swedish Certification Body for IT Security

Certification Report HP SMARTC

Issue: 1.0, 2014-okt-24

Authorisation: Jerry Johansson, Lead Certifier , 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. Six printer versions are included in the scope of the evaluation: the HP LaserJet Enterprise Printer M712 and M806 Series, the HP Color LaserJet Enterprise Printer M651, M750, and M855 Series, and the HP OfficeJet Enterprise Color Printer X555 Series. The network connections and the print jobs are protected by encryption. In the evaluated configuration, print jobs are stored in encrypted form and printed from the control panel later.

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 is outside the scope of the evaluation, but the effect of cryptographic function calls from the TOE has been verified. 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-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B

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

2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B

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

2600.2-SCN, SFR Package for Hardcopy Device Scan 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 was completed on the 10th of October 2014. 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.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2014002
Name and version of the certified IT product and the TOE	HP LaserJet Enterprise Printer M712 Series (M712xh, M712dn, M712n) System firmware version 2302786_433714 JetDirect firmware version JDI23230013 HP LaserJet Enterprise Printer M806 Series (M806+, M806+ NFC/Wireless Direct, M806dn) System firmware version 2302786_433710 JetDirect firmware version JDI23230013 HP Color LaserJet Enterprise Printer M651 Series (M651xh, M651dn, M651n) System firmware version 2302786_433707 JetDirect firmware version JDI23230013 HP Color LaserJet Enterprise Printer M750 Series (M750xh, M750dn, M750n) System firmware version 2302786_433728 JetDirect firmware version JDI23230013 HP Color LaserJet Enterprise Printer M855 Series (M855xh, M855dn, M855+ NFC/Wireless Direct) System firmware version 2302786_433709 JetDirect firmware version JDI23230013 HP OfficeJet Enterprise Color Printer X555 Series (X555xh, X555dn) System firmware version 2302786_433705 JetDirect firmware version JDI23230013
Security Target	Hewlett-Packard LaserJet Enterprise Printer M712 Series, LaserJet Enterprise Printer M806 Series, Color LaserJet Enterprise Printer M651 Series, Color LaserJet Enterprise Printer M750 Series, Color LaserJet Enterprise Printer M855 Series, and OfficeJet Enterprise Color Printer X555 Series Firmware with Jetdirect Inside Security Target, Hewlett Packard, 2014-10-14, document version 2.0
Assurance level	EAL 2 + ALC_FLR.2

Sponsor	Hewlett Packard
Developer	Hewlett Packard
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Recognition scope	CCRA, SOGIS, EA/MLA
Certification date	2014-10-23

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptography
- Control Panel Identification and Authentication
- IPsec 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 performs auditing of security relevant functions. 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 QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec. The TOE supports the decrypting of print jobs encrypted using the Job Encryption Password. The corresponding decryption functionality is included in the TOE.

3.3 Control Panel Identification and Authentication

The Control Panel interface supports both local and remote sign in methods. The following sign in methods are allowed with the evaluated configuration:

- Local sign in method:
  - Local Device Sign In, using a local user database
- Remote sign in methods:
  - LDAP Sign In
  - Windows Sign In (via Kerberos)

Local Device Sign In is only available through the Control Panel. The TOE contains a local user database for defining non-administrative (U.NORMAL, by default) device user accounts used to support the Local Device Sign In mechanism. Each device user account contains the following security attributes:

- Access Code (8 digits)
- Display Name
- Permission Set

The Access Code is a number that serves as both the login user identifier and the authentication secret. Each user's Access Code is unique from all other Local Device users. In the evaluated configuration, the Access Code length must be 8 digits.

The Display Name is a unique name assigned to the account by the administrator. This name is a security attribute because it is used in audit records to identify the user. (The Access Code is not written in the audit records.)

The Permission Set defines/determines a user's access to many of the TOE's functions.

Like Local Device Sign In, the remote sign in methods are only used by the Control Panel. The TOE receives authentication credentials from the Control Panel users and passes the credentials to the remote sign in method. The remote sign in method returns an authentication decision to the TOE. This decision is then enforced by the TOE by granting or denying access to the Control Panel user.

In the case of LDAP, the user name and password entered at the Control Panel are used to bind to the LDAP server. The user must have a valid and active LDAP account in order to successfully bind using this method.

In the case of Kerberos, the user name and password entered at the Control Panel are used to authenticate with the Windows domain controller. The user must have a valid and active Windows domain account in order to successfully bind using this method.

3.4 IPsec Identification and Authentication

The TOE uses IPsec to identify and mutually authenticate the following user types:

- Administrative Computer (U.ADMINISTRATOR)
- Network Client Computers (U.NORMAL) IPsec uses IP addresses and X.509v3 certificates via the IKE protocols (IKEv1 and IKEv2) to identify and authenticate, respectively, a client computer.

The User Identity of a client computer is its IP address. The TOE's internal firewall maintains lists (IPsec/Firewall address templates) of IP addresses of client computers that can connect to the TOE as a Network Client Computer and as the Administrative Computer. If a client computer has an unrecognized IP address that is not defined in the IPsec/Firewall as either the Administrative Computer or a Network Client Computer, then the client computer is not allowed to connect to the TOE. Similarly, if the client computer presents an invalid or unknown (unrecognized CA) X.509v3 certificate, the IPsec mutual authentication mechanism will fail.

The TOE also uses IP addresses and X.509v3 certificates via the IKE protocols to connect to and identify other trusted IT products.

Both the Administrative Computer and the Network Client Computers can access the PJL Interface on port 9100, but only the Administrative Computer can access the EWS (HTTP) interface, Web Services interface (OXPd and WS-*), and SNMP interface.

3.5 Data Protection and Access control

● Permission Sets - For Control Panel users, the TOE uses a user's User Role (as determined by each user's Permission Set) to determine a user's access to many TOE functions. Only U.ADMINISTRATOR can create, modify, and delete Permission Sets.

● Job PINs - Users can control access to each print job that they place under the TOE's control by assigning a Job PIN to each job. A Job PIN limits access to a stored print job while the job resides under the TOE's control and allows a user to control when the job is printed so that physical access to the hard copies can be controlled by the user. A Job PIN must be 4 digits (0000-9999) in length. Only one Job PIN is permitted per job.

● Job Encryption Password - The TOE can store and decrypt encrypted stored print jobs received from a client computer. A stored print job is first encrypted by the client computer using a user-specified Job Encryption Password and AES-256 in CBC mode. The job is then sent encrypted to the TOE and stored encrypted by the TOE. To decrypt the job, a Control Panel user must enter the correct Job Encryption Password used to encrypt the job. The decryption algorithm is included in the TOE. Only one Job Encryption Password is permitted per job.

● Common access control - The TOE protects each print job in Job Storage from non-administrative users through the use of a user identifier and a Job PIN or through the use of a Job Encryption Password. The user identifier for a print job received from a client computer is either assigned by that client computer or assigned by the user sending the print job from the client computer. Every print job in Job Storage is assigned either a Job PIN or a Job Encryption Password by the user at job creation time. If the TOE receives a print job from a client computer without either a Job PIN or a Job Encryption Password, the TOE cancels the job.

● TOE function access control - The TOE controls Control Panel access to TOE functions through the use of Permission Sets. The home screen sign in process assigns the Permission Set to the authenticated user's session. This session Permission Set becomes the user's User Role. Access to each TOE device function is configurable in a Permission Set by an administrator. A user can perform any function permitted in the Permission Set. Control Panel applications (e.g., Print) use the user's Permission Set to determine which of the application's functions should be allowed or disallowed for the user. A Control Panel user can perform the [PP2600.2] functions of F.DSR, F.PRT and F.SMI as determined by the user's Permission Set.

● Residual Information Protection - Objects that are deleted in the TOE are made unavailable to TOE users preventing TOE users from recovering the contents of deleted objects.

3.6 Protection of the TSF

● Restricted Forwarding of Data to external interfaces - The TOE does not allow forwarding of data to an external interface. The TOE contains only one external interface in the evaluated configuration and that interface is the Shared-medium Interface.

● TSF Self-Testing - The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of correct operations tests, TSF Data integrity tests, and integrity tests of TSF executable code.

● Reliable Timestamps - The TOE contains a system clock which is used to generate reliable time stamps.

3.7 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 system. The inactivity period is managed by the administrator via EWS (HTTP) or with WS-* web services.

3.8 Trusted Channel Communication and certificate management

The TOE supports the following mechanisms to protect data transferred over the Shared-medium interface:

● IPsec with X509v3 certificates, along with certificate management for adding, replacing, and deleting certificates.

● Kerberos protected by IPsec.

3.9 User and Access Management

The TOE supports the following types of users; administrators and users. These users have the following management capabilities:

● Administrators - manage the security functionality of the printer and manage users.

● Users - manage user data which they have access to.

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 organisation, and are trained and competent to follow those policies and procedures.

A.ADMIN.TRAINING - Administrators are aware of the security policies and the procedures of their organisation, and 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

Seven 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 authorised administrator has access to it.

A.USER.PC.POLICY - User computers are configured and used in conformance with the organisation's security policies.

A.DNS.RELIABLE - When the TOE resolves network hostnames to addresses with the Domain Name System, the Domain Name System provides reliable network addresses.

A.NTP.RELIABLE - When the TOE synchronizes time with the Network Time Protocol server, the Network Time Protocol server provides reliable time synchronization information.

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

A.WINS.RELIABLE - When the TOE resolves network hostnames to addresses with the Windows Internet Name Service, the Windows Internet Name Service provides reliable network addresses.

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 unauthorised persons.

T.DOC.ALT - User Document Data may be altered by unauthorised persons.

T.FUNC.ALT - User Function Data may be altered by unauthorised persons.

T.PROT.ALT - TSF Protected Data may be altered by unauthorised persons.

T.CONF.DIS - TSF Confidential Data may be disclosed by unauthorised persons.

T.CONF.ALT - TSF Confidential Data may be altered by unauthorised 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 printing and storing print jobs. It can be connected to a local network through the embedded Jetdirect Inside print server's built-in Ethernet

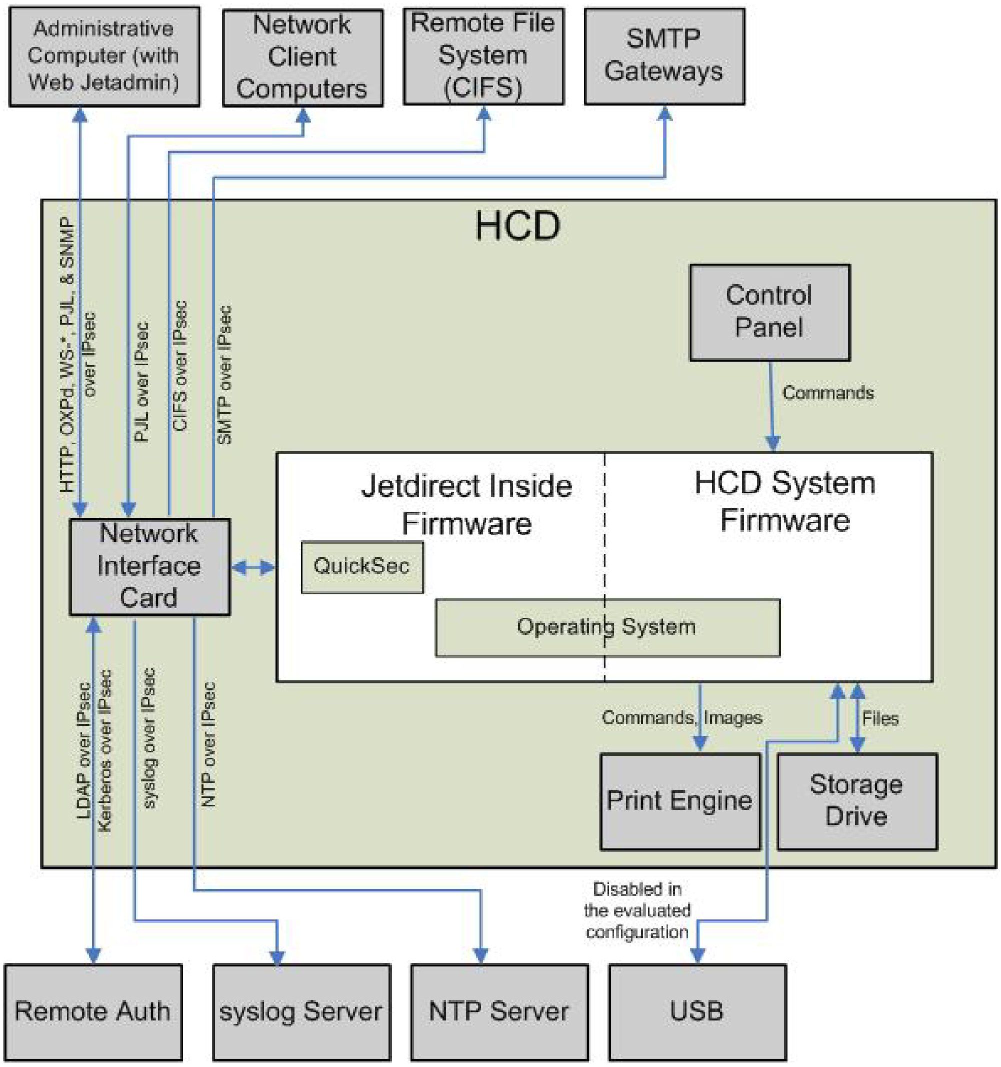

Figure 1: HCD physical diagram

Figure 1 shows a high-level physical diagram of an HCD (hardcopy device)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 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 this Security Target, 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 in the operational environment 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) an encrypted job from a client 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 Common Internet File System (CIFS) protocol. CIFS 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 CIFS through the TOE. The connection is protected using IPsec.

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. Depending on the model, the Control Panel may have a 4-line, non-touchscreen display (M712 and M750) or a 4.3-inch 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 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.

6 Documentation

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

HP Color LaserJet Enterprise M651 User Guide [UG651]

HP LaserJet Enterprise 700 M712 User Guide [UG712]

HP Color LaserJet Enterprise M750 Printer Series User Guide [UG750]

HP LaserJet Enterprise M806 User Guide [UG806]

HP Color LaserJet Enterprise M855 User Guide [UG855]

HP Officejet Enterprise Color X555 User Guide [UG555]

TOE Download Instructions [Download]

Common Criteria Evaluated Configuration Guide for HP Single-Function Printers [CCcfg]

7 IT Product Testing

7.1 Developer Testing

The developer performed extensive 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 six hardcopy devices. The developer testing was performed in the developer's premises in Boise, Idaho, USA.

7.2 Evaluator Testing

The evaluators focused on two of the hardcopy devices (M806 and X555), which were tested in the developer's premises in Boise, Idaho, USA.

The evaluators used the developer's test setup and verified a sample of the developer's test cases.

The evaluators also devised and performed additional test cases to provide improved coverage of the security functions and the 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 M806 in Boise, Idaho.

8 Evaluated Configuration

The TOE shall run on either the M651, M750, M855, M712, M806 or the X555 hardcopy device. The correct firmware versions for each hardware is listed in section 2 Identification.

The TOE shall be configured in accordance with the CC Configuration Guide [CCcfg]. In particular:

- HP High Performance Secure Hard Disk, if installed, must be configured with a password to activate drive encryption
- Device Administrator Password must be set
- 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 authentica tion using Kerberos or Pre-Shared Key is not supported)
- IPsec Authenticated Headers (AH) must be disabled
- IPsec IKE Main Mode for key exchange must be used
- 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 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
- 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 the [ST].

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
HP	Hewlett-Packard
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
MFP	Multifunction Product
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	Hewlett-Packard LaserJet Enterprise Printer M712 Series, LaserJet Enterprise Printer M806 Series, Color LaserJet Enterprise Printer M651 Series, Color LaserJet Enterprise Printer M750 Series, Color LaserJet Enterprise Printer M855 Series, and OfficeJet Enterprise Color Printer X555 Series Firmware with Jetdirect Inside Security Target, Hewlett Packard, 2014-10-07, document version 2.0
UG651	HP Color LaserJet Enterprise M651 User Guide, Hewlett-Packard, April 2014, Edition 1
UG712	HP LaserJet Enterprise 700 M712 User Guide, Hewlett-Packard, November 2012, Edition 2
UG750	HP Color LaserJet Enterprise M750 Printer Series User Guide, Hewlett-Packard, October 2013, Edition 1
UG806	HP LaserJet Enterprise M806 User Guide, Hewlett-Packard, October 2013, Edition 1
UG855	HP Color LaserJet Enterprise M855 User Guide, Hewlett-Packard, November 2013, Edition 1
UG555	HP Officejet Enterprise Color X555 User Guide, Hewlett-Packard, April 2014, Edition 1
CCcfg	Common Criteria Evaluated Configuration Guide for HP Single Function Printers, Hewlett-Packard, 2014-05-23, Edition 1
Download	Common Criteria Certification for HP LaserJet Printers, Hewlett-Packard, 2014-06-16
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, 2013-09-30, document version 20.0

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 2014-04-08:

QMS 1.16.1	valid from 2014-02-27
QMS 1.16.2	valid from 2014-07-07

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 1.16.2”.

The certifier concluded that, from QMS 1.16.1 to the current QMS 1.16.2, there are no changes with impact on the result of the certification.