Swedish Certification Body for IT Security

Certification Report HP MFP M4555 and CM4540

Issue: 1.0, 2014-feb-05

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is the firmware of a multifunction printer, MFP, with the exception of the operating system and the crypto module implementation. Two versions of the multifunction printer are included in the scope of the evaluation: the LaserJet M4555 MFP (black and white) and the Color LaserJet CM4540 MFP (color). These multifunction printers provide fax, copying, scanning, and network printing functionality. The network connections and the print jobs are protected by encryption, and stored jobs may be printed or sent by e-mail, to FTP or HTTP servers or to a network hard drive.

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 19th of December 2013. 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, and by observing the evaluators during testing. 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 4 + 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	CSEC2012003
Name and version of the certified IT product and the TOE	HP LaserJet M4555 MFP with MFP firmware version 2204045_233103 JetDirect firmware version JDI22210024.FF HP Color LaserJet CM4540 MFP with MFP firmware version 2204045_233099 JetDirect firmware version JDI22210024.FF
Security Target	Hewlett-Packard LaserJet M4555 MFP Series and Color LaserJet CM4540 MFP Series with JetDirect Inside Security Target, Hewlett Packard, 2014-01-22, 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
Certification date	2014-02-05

3 Security Policy

The TOE provides the following security services:

- Auditing
- 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 provides means to generate audit records for security relevant events.

3.2 Identification and Authentication

Console access requires user identification and authentication.

3.3 Data Protection and Access Control

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

3.4 Protection of the TSF

Restricted forwarding - the administrator may restrict the automatic forwarding of data, specifically fax forwarding and fax archiving.

The TOE contains a suite of self tests to verify the integrity of specific TSF data and the TOE executables.

In the evaluated configuration, the TOE system clock will synchronise with an NTP server.

3.5 TOE Access Protection

Control panel access is protected by administrator configurable inactivity timeout and an administrator selectable automatic logout after a user job has been started.

3.6 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.

3.7 User and Access Management

An administrator has 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 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 is configured to use the Network Time Protocol as a time synchronisation source, the Network Time Protocol provides a reliable time synchronisation source for the TOE.

A.SERVICES.RELIABLE - When the TOE uses any of the network services Kerberos, 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 multifunction printer designed to be shared by many client computers and human users. It performs the functions of copying, faxing, printing, and scanning of documents. It can be connected to a local network through the embedded Jetdirect Inside print server's built-in Ethernet, to an analog phone 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).

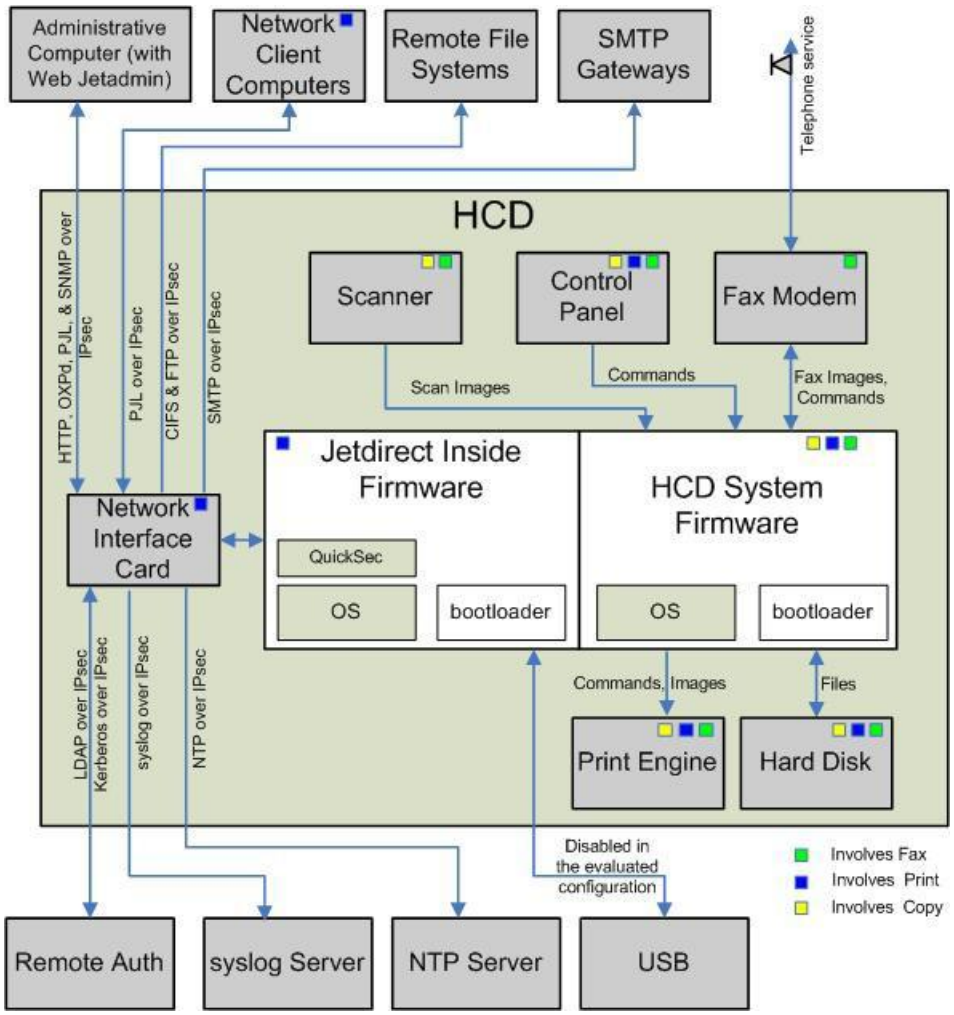

Figure 1: HCD physical diagram

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

6 Documentation

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

HP Color LaserJet Enterprise CM4540 Series - Users Guide [UG4540]

HP LaserJet Enterprise M4555 Series - Users Guide [UG4555]

TOE Download Instructions [Download]

Common Criteria Evaluated Configuration Guide for HP LaserJet MFPs - HP Color LaserJet CM4540 MFP Series and HP LaserJet M4555 MFP Series [CCcfg]

Common Criteria Administrator Operational Guide for HP LaserJet MFPs - HP Color LaserJet CM4540 MFP Series and HP LaserJet M4555 MFP Series [CCadm]

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 both hardcopy devices (CM4540 and M4555). The developer testing was performed in the developer's premises in Boise, Idaho, USA.

7.2 Evaluator Testing

The evaluators focused on one of the hardcopy devices (M4555), which was tested in the evaluation facility's premises in Stockholm, Sweden. The evaluators arranged a test setup similar to the developer's and verified a sample of the developer's test cases.

The evaluators also devised and performed additional test cases to provide a full cover 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 vulnerability scans of the network interface of the TOE, covering TCP and UDP ports both for IP v.4 and IP v.6. Testing was performed on the hardcopy device M4555.

8 Evaluated Configuration

The TOE shall run on either the CM4540 or the M4555 hardcopy device, and shall be configured in accordance with the CC Configuration Guide [CCcfg].

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
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 M4555 MFP Series and Color LaserJet CM4540 MFP Series with JetDirect Inside Security Target, Hewlett Packard, 2014-01-22, document version 2.0
UG4540	HP Color LaserJet Enterprise CM4540 Series - Users Guide, Hewlett Packard, October 2010, edition 2
UG4555	HP LaserJet Enterprise M4555 Series - Users Guide, Hewlett Packard, April 2011, edition 2
CCcfg	Common Criteria Evaluated Configuration Guide for HP LaserJet MFPs - HP Color LaserJet CM4540 MFP Series and HP LaserJet M4555 MFP Series, Hewlett Packard, December 2013, edition 2
CCadm	Common Criteria Administrator Operational Guide for HP LaserJet MFPs - HP Color LaserJet CM4540 MFP Series and HP LaserJet M4555 MFP Series, Hewlett Packard, December 2013, edition 2
Download	Common Criteria Certification for HP LaserJet Printers, Hewlett Packard, 2013-08-22
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, 2013-07-17, document version 19.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2013-06-18, document version 4.0