Swedish Certification Body for IT Security

Certification Report- Lexmark MFP wHD

Issue: 1.0, 2016-mar-11

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The TOE is the firmware of Lexmark's Multi Function Printers MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, MX910, MX911, MX912, XM7155, XM7163, XM7170, XM9145, XM9155, XM9165, CX510h and XC2132. All equipped with hard disk.

Firmware versions:

- LW50.SB4.P555: MX511h
- LW50.SB7.P555: MX611h
- LW50.TU.P555: MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170
- LW50.MG.P555: MX910, MX911, MX912, XM9145, XM9155, XM9165
- LW50.GM7.P555: CX510h and XC2132

Conformance is claimed to PP Identification: 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A, version 1.0, dated January 2009 PP Conformance:

- PP Conformance:
- "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A," "2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A,"
- "2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A,"
- "2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A," "
- 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A," and
- "2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A"

This Security Target claims demonstrable conformance to the Security Problem Definition (APE_SPD), Security Objectives (APE_OBJ), Extended Components Definitions (APE_ECD), and the Common Security Functional Requirements (APE_REQ) of the referenced PP.

This TOE performs the functions F.PRT, F.SCN, F.CPY, F.FAX, and F.SMI as defined in the referenced PP and claims demonstrable conformance to the augmented SFR packages defined for each of these functions.

The evaluation has been performed by Combitech AB and EWA-Canada. 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 EAL3, augmented by ALC_FLR.2.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

EWA-Canada operates as a Forign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

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 3 + ALC_FLR.2.

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

The invocation of cryptographic primitives has been included in the scope of this evaluation, while correctness of implementation of cryptographic primitives been excluded from the TOE. Correctness of implementation is done by vendor affirmation through CAVP certification referred to in the Security Target. Users of this product is advised to consider their acceptance of this affirmation.

2 Identification

Certification Identification	
Certification ID	CSEC2015006
Name and version of the certified IT product	Firmware for Multi-Function Devices (Printers) Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, MX910, MX911, MX912, XM7155, XM7163, XM7170, XM9145, XM9155, XM9165, CX510h and XC2132 Firmware versions: • LW50.SB4.P555: MX511h • LW50.SB7.P555: MX611h • LW50.TU.P555: MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170 • LW50.MG.P555: MX910, MX911, MX912, XM9145, XM9155, XM9165 • LW50.GM7.P555: CX510h and XC2132
Security Target Identification	Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, MX910, MX911, MX912, XM7155, XM7163, XM7170, XM9145, XM9155, XM9165, CX510h and XC2132 Multi-Function Printers Security Target [ST].
EAL	EAL3+ ALC_FLR.2. CCRA recognition for components up to EAL 2 and ALC_FLR only
Sponsor	Lexmark International Technologies S.A.
Developer	Lexmark International Technologies S.A.
ITSEF	Combitech AB
Common Criteria version	3.1, revision 4
CEM version	3.1, revision 4
Certification completion date	2016-03-11

3 Security Policy

The TOE consists of ten security functions. Below is a short description of each of them. For more information, see Security Target [ST]

Audit Generation	The TOE generates audit event records for security-relevant events. A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated.
Identification and Authentication	Users are required to successfully complete the I&A process before they are permitted to access any restricted functionality. The set of restricted user functionality is under the control of the administrators, with the exception of submission of network print jobs which is always allowed. Users are permitted to access any TOE functionality that has a corresponding access configured for “no security”.
Access Control	Access control validates the user access request against the authorizations configured by administrators for specific functions. On a per-item basis, authorization may be configured as “disabled” (no access), “no security” (open to all users), or restricted (via security templates) (some items do not support all three options).
Management	The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. Authorization is granular, enabling different administrators to be granted access to different TSF data. When an administrator modifies TSF data, an audit record is generated.
Operator Panel Lockout	The Operator Panel Lockout function enables the touch panel to be “locked” to prevent anyone from using it until it is “unlocked” by an authorized user. This function is enabled when a security template is associated with the Operator Panel Lock access control described above. When enabled, an icon is displayed on the Home page to lock the panel.
Fax Separation	The Fax Separation security function assures that the information on the TOE, and the information on the network to which the TOE is attached, is not exposed through the phone line that provides connectivity for the fax function. This function assures that only printable documents are accepted via incoming fax connections, and that the only thing transmitted over an outgoing fax connection (in the evaluated configuration) is a document that was scanned for faxing.
Hard Disk Encryption	All user data saved on the Hard Disk is encrypted using 256-bit AES. The types of data saved on the Hard Disk (and therefore encrypted) include buffered job data, held jobs, images referenced by other jobs, and macros. The contents of each file are automatically encrypted as they are written to the Hard Disk and automatically decrypted when the contents are read. This security function is intended to protect against data disclosure if a malicious agent is able to gain physical possession of the Hard Disk. This security function operates transparently to users and is always enabled in the evaluated configuration.

Disk Wiping	In the evaluated configuration, the TOE is configured to perform automatic disk wiping with a multi-pass method. Files containing user data are stored on the internal hard drive until they are no longer needed. At that time, they are logically deleted and marked as needing to be wiped. Until the wiping occurs, the disk blocks containing the files are not available for use by any user. Every 5 seconds, the TOE checks to see if any “deleted” files are present and begins the disk wiping process.
Secure Communications	IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are TDES and AES. SHA is supported for HMACs.
Self Test	During initial start-up, the TOE performs self tests on the hardware. The integrity of the security templates and building blocks is verified by ensuring that all the security templates specified in access controls exist and that all building blocks referenced by security templates exist. The integrity of the stored TSF executable code by calculating a hash of the executable code and comparing it to a saved value.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following assumption about the usage are made:

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.USER.TRAINING TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

4.2 Environmental Assumptions

The following assumption about the environment are made:

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.IPSEC IPSec with ESP is used between the TOE and all remote IT systems with which it communicates over the network using IPv4 and/or IPv6.

4.3 Clarification of Scope

Four categories of threat agents are defined:

- Persons who are not permitted to use the TOE who may attempt to use the TOE.
- Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
- Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.
- Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The identified threats against the TOE are listed below:

- T.CONF.ALT TSF Confidential Data may be altered by unauthorized persons
- T.CONF.DIS TSF Confidential Data may be disclosed to unauthorized persons
- T.DOC.ALT User Document Data may be altered by unauthorized persons
- T.DOC.DIS User Document Data may be disclosed to 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

Four Organisational Security Policies are defined.

- P.AUDIT.LOGGING To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel

- P.INTERFACE.MANAGEMENT To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
- P.SOFTWARE.VERIFICATION To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
- P.USER.AUTHORIZATION To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner

5 Architectural Information

5.1 TOE Design

The following TOE model is adapted from the Protection Profile, ref. [PP].

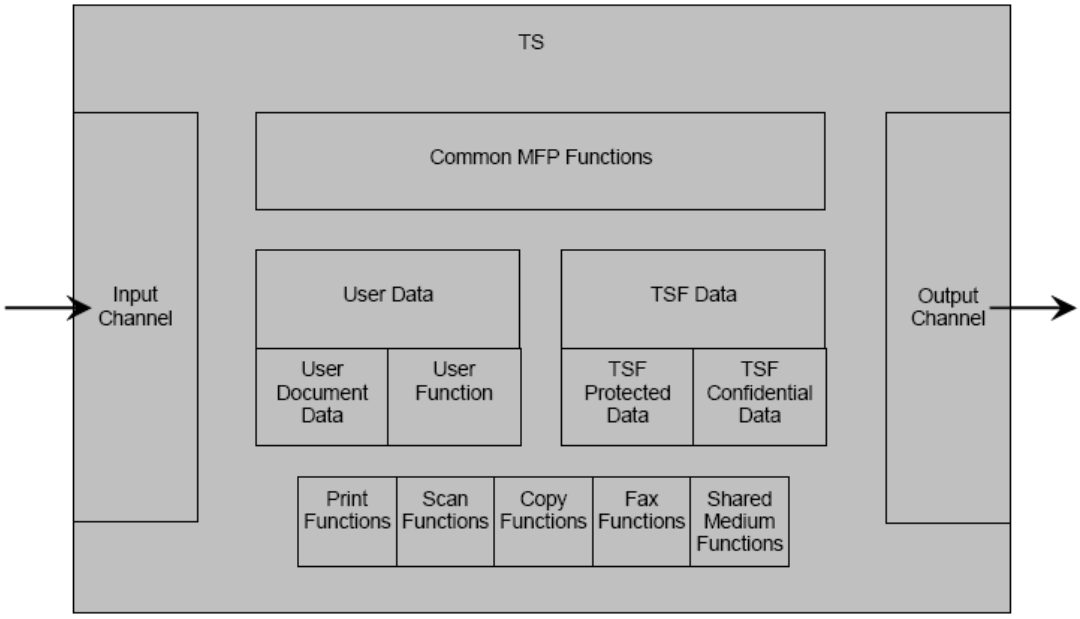

Figure 1, TOE model

The TOE is comprised of the following subsystems:

Operating System

The Operating System subsystem provides standard operating system services such as file system, process management, timers and memory management. The memory management functionality zeroizes buffers in memory upon deallocation.

The Operating System subsystem executes a series of self-tests of the MFP upon each start-up of the system. This subsystem also maintains the system time, which is used to insert timestamps into audit records when they are generated.

GUI Manager

The GUI Manager subsystem handles all interactions with local users via the touch screen and keypad. This subsystem retrieves (from the Object Store subsystem) and displays the appropriate information on the touch screen and processes input from the touch screen and keypad. When configuration changes are made, the updated information is sent to the Object Store subsystem to be saved and acted on.

User Authentication

The User Authentication subsystem handles all validation of user credentials and authorizations, whether the validation is performed locally or remotely. When credentials or authorization checks are received from the GUI Manager or Web Server subsystems, User Authentication retrieves information from Object Store to determine if local, remote, or PKI validation should be performed.

Object Store

The Object Store subsystem is responsible for managing the storage of configuration parameters, forwarding audit records between the generating subsystem and the Audit subsystem, and forwarding user jobs between the receiving subsystem and the destination subsystem. This subsystem also maintains a list of pending user jobs.

Audit

The Audit subsystem is responsible for formatting audit information into the standard Syslog format, inserting a timestamp, and forwarding the audit records to the configured Syslog server. If NTP is configured, this subsystem also interacts with the configured NTP server(s) to maintain the system time.

Network Interface

The Network Interface subsystem is responsible for all interactions with the Network Interface Card and provides all the processing of network protocol layers that are common to multiple software subsystems (e.g. TCP, IP, IPSec). This subsystem interacts with remote IT systems via the network protocols. Since cryptography is required for several of the network protocols to establish trusted channels, this subsystem participates in key management functions and invokes the Crypto Library subsystem to perform cryptographic operations. All communication with remote IT systems is required to use IPSec.

Print

The Print subsystem processes received print jobs from the network interface, scanner and fax line (via the Object Store subsystem). Received network print jobs are queued to be deleted after the print job expiration timeout if they do not contain a PJL SET USERNAME statement. Audit information is generated as jobs are received, indicating the job is created. The user jobs are converted to raster images and queued for printing. The list of user jobs waiting to be printed is communicated to the Object Store subsystem. Audit information is generated as jobs are completed.

Scan Manager

The Scan Manager subsystem is responsible for controlling the operation of the scanner hardware and formatting the scanned images into an appropriate format. This subsystem invokes the Operating System subsystem to save the user data on the hard drive in encrypted form. The format may be an email message with an attachment for scan-to-email operations or scan-to-fax operations (when fax server is configured), or raster image for copy operations or scan-to-fax operations (when analog fax is configured). The currently logged in user on the touch screen is the user associated with the job. Once formatted, the user job is sent to the Object Store subsystem for delivery to the destination subsystem.

Email

The Email subsystem is responsible for forwarding user jobs to a remote IT system via SMTP. In the evaluated configuration, the user jobs may have originated from a scan-to-email operation or a scan-to-fax operation with the fax server configured. The Operating System subsystem is invoked to open the file containing the user data and decrypt it. When the user job has been forwarded, the Operating System subsystem is invoked to delete the file containing the user data and wipe the area of the hard disk on which the data was stored. Audit information is generated upon job completion and forwarded to the Audit subsystem via the Object Store subsystem.

Web Server

The Web Server subsystem is responsible for providing user access to TOE functions from remote IT systems via browser sessions. This subsystem retrieves (from the Object Store subsystem) and presents the appropriate information for display. When configuration changes are made, the updated information is sent to the Object Store subsystem to be saved and acted on.

Fax

The Fax subsystem is responsible for controlling the operation of the fax modem hardware. For incoming faxes, this subsystem invokes the Operating System subsystem to save the user data as a raster image on the hard drive in encrypted form. Unprocessed data is never accepted by this subsystem and the evaluated configuration does not permit unprocessed data received via the fax line to be forwarded out the Network Interface Card. The touch screen user that releases the held faxes is the user associated with the job. Once complete, the user job is sent to the Object Store subsystem for delivery to the Print subsystem.

Crypto Library

The Crypto Library subsystem provides cryptographic algorithm support used by other subsystems to perform cryptographic operations. The operations supported include encryption, decryption, hashing, message authentication coding, digital signatures and random number generation.

6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

1. Lexmark Common Criteria Installation Supplement and Administrator Guide
2. Lexmark Embedded Web Server – Security Administrator's Guide
3. Lexmark MX410 and MX510 Series User's Guide
4. Lexmark MX610 Series User's Guide
5. Lexmark MX710 Series User's Guide
6. Lexmark MX810 Series User's Guide
7. Lexmark XM7100 Series User's Guide
8. Lexmark CX510 Series User's Guide
9. Lexmark XC2132 User's Guide
10. Lexmark MX910 Series User's Guide
11. Lexmark XM9100 Series User's Guide

7 IT Product Testing

7.1 Developer Tests

The developer performed manual tests. The developer's testing covers the security functional behaviour of all TSFIs and SFRs as well as the interactions of the subsystems.

7.2 Independent Evaluator Tests

The evaluator's independent tests were chosen to complement the developer's manual tests in covering as much of the security functional behavior of the TSFIs and SFRs.

The evaluator repeated all of the developer's test cases and performed the individual and penetration test cases. The tests included:

- TOE Installation
- Identification and Authentication
- Access Control and Management
- Touch Panel Lockout
- Hard Disk Encryption and Disk Wiping
- Trusted Channel
- Repetition of Developer's Testing

The evaluator used a similar test configuration as the developer consisting of :

- TOE: MX611de without Smart Card reader
- Workstation: Windows client used to send print jobs to the TOE, open browser sessions to manage the TOE, and to exchange email with the Email Server.
- Primary Domain Controller: Windows server providing Active Directory, DNS, Kerberos, GSSAPI, PKI and NTP services
- Email Server: SMTP server capable of receiving email from the TOE and forwarding it to a user on Workstation
- Syslog Server: Capable of receiving and diaplaying Syslog messages from the TOE
- Network Monitor: Used to display and analyse network traffic
- Fax: Analog fax machine
- IP Network
- Phone network

The tests were run manually from the MFP's touch screen, the Embedded Web Server, and the workstation.

Repetition of the developer's test cases was done at the developer's site in Lexington, USA.

The actual results of all test cases were consistent with the expected test results and all tests were judged to pass.

7.3 Penetration Tests

Four types of vulnerability tests were performed:

- Port scan
- Vulnerability scan

- Communication protocol compliance
- Hard disk encryption verification

Port scans were run after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nessus (www.tenable.com) basic network vulnerability scans were run. No high severity issues were found.

It was verified that all traffic to and from the Primary Domain Controller was using IPSec in ESP mode. It was also verified that no down negotiating to weaker algorithms than specified for the trusted channel is possible.

The hard disk was examined to verify that all user data stored for held printing, scanning, and incoming fax is encrypted.

Search in public sources revealed 15 vulnerabilities with CVE ids remaining in the TOE. The vulnerabilities were however deemed not to be exploitable through source code analysis and tests.

All penetration testing had negative outcome, i.e. no exploitable vulnerabilities were found.

8 Evaluated Configuration

8.1 Dependencies to Other Hardware, Firmware and Software

The TOE is the firmware of an MFP. The MFP hardware must be one of the models supported for the firmware versions specified for the TOE. To be fully operational, any combination of the following items may be connected to the MFP:

- A LAN for network connectivity. The TOE supports IPv4 and IPv6.
- A telephone line for fax capability.
- IT systems that submit print jobs to the MFP via the network using standard print protocols.
- IT systems that send and/or receive faxes via the telephone line.
- An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
- LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
- Card reader and cards to support Smart Card authentication using Common Access Card (CAC) or Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card readers are:
  - Omnikey 3121 SmartCard Reader,
  - Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),
  - SCM SCR 331,
  - SCM SCR 3310v2.

8.2 Excluded from the TOE Evaluated Configuration

The following features of the TOE are outside of or not allowed in the evaluated configuration.

- Support for
  - Optional network interfaces.
  - Optional parallel or serial interfaces.
  - USB ports on the MFPs that perform document processing functions.
- Support for AppleTalk.
- Other I&A mechanisms than Internal Accounts, LDAP+GSSAPI on a per-user basis, the Backup Password mechanism, and Smart Card authentication.
- Other eSF, Java applications, than “eSF Security Manager”, “Smart Card Authentication”, “Secure Held Print Jobs”, “Smart Card Authentication Client”, “PIV Smart Card Driver (if PIV cards are used)”, “CAC Smart Card Driver (if CAC cards are used)”, and “Background and Idle Screen”.
- Fax forwarding.
- Simple Network Management Protocol (SNMP).
- Internet Printing Protocol (IPP).

9 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
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
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Authrisation controls	ALC_CMC.3	Pass
Implementation representation CM coverage	ALC_CMS.3	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Flaw reporting procedures	ALC_FLR.2	Pass
Development	ADV	Pass
Security Architecure description	ADV_ARC.1	Pass
Functional specification with complete summary	ADV_FSP.3	Pass
Architecual design	ADV_TDS.2	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: Basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Vulnerability analysis	AVA_VAN.2	Pass

10 Evaluator Comments and Recommendations

Software components with known vulnerabilities are included in the TOE. It is not known if the software in the TOE environment is vulnerable to these vulnerabilities. The developer attests that they have used public information and testing to attempt to exploit the potential vulnerabilities, but have been unable to launch successful attacks.

The evaluator has reviewed the developer's analysis and test results. The evaluator has also repeated developer tests and performed own testing. to confirm the results. The calculated attack potential for these vulnerabilities is out of the range specified for EAL3 evaluations. Therefore, it is acceptable for these vulnerabilities to be present in the TOE and they are classified as residual vulnerabilities.

11 Glossary

AD	Active Directory
AES	Advanced Encryption Standard
AIO	All In One
BSD	Berkeley Software Distribution
CAC	Common Access Card
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CM	Configuration Management
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GSSAPI	Generic Security Services Application Program Interface
HTTP	HyperText Transfer Protocol
I&A	Identification & Authentication
IPP	Internet Printing Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6.	Internet Protocol version 6
ISO	International Standards Orgaization
IT	Information Technology
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
KDC	Key Distribution Center
KDF	Key Derivation Function
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	MegaByte
MFD	Multi-Finction Device
MFP	Multi-Function Printer
NTP	Network Time Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification

PJL	Printer Job Language
PP	Protection Profile
RFC	Request For Comments
SASL	Simple Authentication and Security Layer
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[ST] Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, MX910, MX911, MX912, XM7155, XM7163, XM7170, XM9145, XM9155, XM9165, CX510h and XC2132 Multi-Function Printers Security Target, 2015-12-15, document version 1.5

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 2015-06-17:

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

QMS 1.19 valid from 2016-02-05

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 1.19”.

The certifier concluded that, from QMS 1.17.3 to the current QMS 1.19, there are no changes with impact on the result of the certification.