Swedish Certification Body for IT Security

Certification Report Lexmark MFD NoHD

Issue: 1.0, 2017-mar-09

Authorisation: Imre Juhász, Lead Certifier , CSEC

Report Distribution:

Arkiv

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the firmware of Lexmark's Multi Function Devices (Printers): Lexmark CX725 and XC4140. The TOE running on one of the supported specified hardware models constitutes a Multi-Function Printer (MFP).

Firmware version:

- ATL. 030.079CC: CX725 and XC4140

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

- PRT, SFR Package for Print Functions,
- SCN, SFR Package for Scan Functions,
- CPY, SFR Package for Copy Functions,
- FAX, SFR Package for Fax Functions and
- SMI, SFR Package for Shared-medium Interface Functions

The Security Target (ST) 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.

The 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.

There are five assumptions made in the ST regarding the secure usage and environment of the MFD. The TOE rely on these being met in order to be able to counter the six threats, and to fulfill the four organizational security policy (OSP) in the ST. The assumptions, the threats and the organizational security policies are described in chapter 4 Assumptions and Clarification of Scope.

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 Foreign 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, 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.

2 Identification

Certification Identification	
Certification ID	CSEC2016002
Name and version of the certified IT product	Firmware for Multi-Functional Devices (Printers) Lexmark CX725 and XC4140 Firmware versions: ・ ATL. 030.079CC: CX725h and XC4150
Security Target Identification	Lexmark CX725 and XC4140 Multi-Function Printers Security Target
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	2017-03-15

3 Security Policy

The TOE consists of eight 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 and transmits them to a remote IT system using the syslog protocol.

Identification and Authentication

When a touch panel or web session is initiated, the user is implicitly assumed to be the Guest (default) user. Per the evaluated configuration, the permissions for this user must be configured such that no access to TSF data or functions is allowed. Therefore, the user must successfully log in as a different user before any TSF data or functions may be accessed.

The TOE supports I&A with a per-user selection of Username/Password Accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment). Smart Card authentication may also be specified for users of the touch panel.

Access Control

Access controls configured for functions (e.g. fax usage) and menu access are enforced by the TOE.

Management

Through web browser and touch panel sessions, authorized administrators may configure access controls and perform other TOE management functions.

Fax Separation

The TOE ensures that only fax traffic is sent or received via the attached phone line. Incoming traffic is processed as fax data only; no management access or other data access is permitted. In the evaluated configuration, the only source for outgoing faxes is the scanner.

D.DOC Wiping

In the evaluated configuration, the TOE automatically overwrites RAM used to store user data as soon as the buffer is released.

Secure Communication

The TOE protects the confidentiality and integrity of all information exchanged over the attached network by using IPSec with ESP for all network communication. Cryptographic keys may be generated by the TOE or pre-shared keys may be entered by the administrator.

Self Test

During initial start-up, the TOE performs self tests on its cryptographic components and the integrity of the configuration data.

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.

Nine assumptions on the operational environment are defined, none of them are to be characterized as unusual.

5 Architectural Information

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

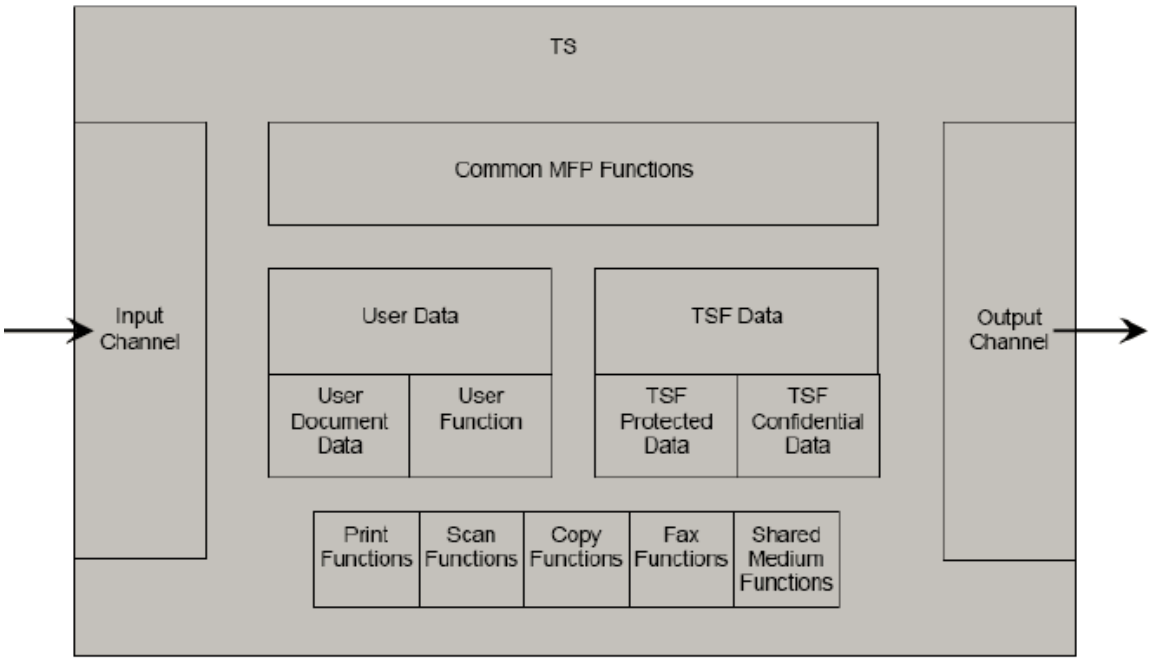

Figure 1, TOE model

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 in memory. 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. When the user job has been forwarded, the Operating System subsystem is invoked to delete the file containing the user data and zeroize the memory in 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 (Remote Management Access (RMA)). 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 in memory. 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:

- Lexmark Common Criteria Installation Supplement and Administrator Guide
- Lexmark Embedded Web Server Administrator's Guide
- Lexmark CX725 Series User's Guide
- Lexmark XC4100 Series User's Guide

7 IT Product Testing

Developer Tests

The developer performed manual tests. The developer's testing covers the security functional behavior of all TSFIs and SFRs as well as the interactions of the subsystems. The developer's testing comprised both firmware and all printer models.

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 developer's test cases and performed individual and penetration tests. The tests included:

- TOE Installation
- Identification and Authentication
- Access Control and Management
- Trusted Channel
- Repetition of Developer's Testing

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

- TOE: CX725 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 displaying 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. The actual results of all test cases were consistent with the expected test results and all tests were judged to pass.

Penetration Tests

The following types of vulnerability tests were performed:

- Port scan
- Vulnerability scan
- PNG fuzzing
- LDAP+GSSAPI authentication down negotiation
- IPSec down negotiation
- IPSec scanning

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.

A scanning tool for network vulnerabilities were run. No high severity issues were found.

A fuzzing tool were used to randomly change the content of a PNG image. The fuzzed images were sent to the MFP for printing.

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, [ST] table 18, is possible.

The IPSec protocol were scanned using an IKE/IPSec scanning tool to reveal unspecified primitives, key lengths, etc.

Search in public sources did not revealed any exploitable or residual vulnerabilities in the TOE including its third party software libraries.

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

8 Evaluated Configuration

In the Security Target [ST] section "1.10 Evaluated Configuration" there are 29 stated configuration options that apply to the evaluated configuration of the TOE. These configuration options need to be set correctly in order to use the evaluated version.

Dependencies to Other Hardware, Firmware and Software

The TOE is the firmware of an MFD. The MFD 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 MFD:

- 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:
  - Identive Cloud 2700 F & Identive Cloud 2700 R readers
  - 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.

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

None

11 Glossary

CAC	Common Access Card
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
GSSAPI	Generic Security Services Application Program Interface
I&A	Identification & Authentication
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
IT	Information Technology
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
MFP	Multi-Function Printer
NTP	Network Time Protocol
OSP	Organizational Security Policy
PJL	Printer Job Language
PIV	Personal Identity Verification
PP	Protection Profile
RAM	Random Access Memory
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Function
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 CX725 and XC4140 Multi-Function Printers Security Target, Lexmark International, Inc., 2017-01-16, document version 1.5
[PP]	2600.1, Protection Profile for Hardcopy Devices, Operational Environment A, dated January 2009, version 1.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.19	2016-02-05	*None*
1.19.1	2016-03-07	*None*
1.19.2	2016-04-28	*None*
1.19.3	2016-06-02	*None*
1.20	2016-10-20	*None*
1.20.1	2017-01-12	*None*
1.21.2	2017-02-27	*None*

A.2 Scheme Notes

Scheme Note 15 - Demonstration of test coverage

Scheme Note 18 - Highlighted Requirements on the Security Target

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 1.20.1".

The certifier concluded that, from QMS 1.19 to the current QMS 1.21.1, there are no changes with impact on the result of the certification.