Swedish Certification Body for IT Security

Certification Report - Lexmark SFP 2017

Issue: 1.0, 2019-jun-18

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the firmware of Lexmark's Function Printers: Lexmark CS622, CS921, CS923, MS622, MS822, and MS826 Single. The TOE running on one of the supported specified hardware models constitutes a Single-Function Printer (SFP).

Firmware versions:

- CSTMH.052.025: CS921, CS923
- CSTZJ.052.025: CS622
- MSTGM.052.025: MS622
- MSTGW.052.025: MS822, MS826

Demonstrable 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,
- 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 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 six 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 5, and the Common Methodology for IT security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL3, augmented by ALC_FLR.3.

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.3.

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	CSEC2017019
Name and version of the certified IT product	Lexmark CS622, CS921, CS923, MS622, MS822, and MS826 Single Function Printers. Firmware versions: - CSTMH.052.025: CS921, CS923 - CSTZJ.052.025: CS622 - MSTGM.052.025: MS622 - MSTGW.052.025: MS822, MS826
Security Target Identification	Lexmark CS622, CS921, CS923, MS622, MS822, and MS826 Single Function Printers Security Target, Lexmark International, Inc., 2018-11-08, version 1.9
EAL	EAL3+ ALC_FLR.3 CCRA recognition for components up to EAL2 and ALC_FLR.3 only.
Sponsor	Lexmark International Technologies S.A.
Developer	Lexmark International Inc.
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1, revision 5
CEM version	3.1, revision 5
QMS version	1.22.3
Scheme Notes Release	14.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2019-06-19

3 Security Policy

The TOE consists of seven 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 other than print job submission (job submission is authorized regardless of what user is logged in). Therefore, the user must successfully log in as a different user before any TSF data or functions other than print job submission 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 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.

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.

A.VIPER The Lexmark Secure Element provides entropy of adequate quality for secure operation of the TOE's DRBG.

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

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

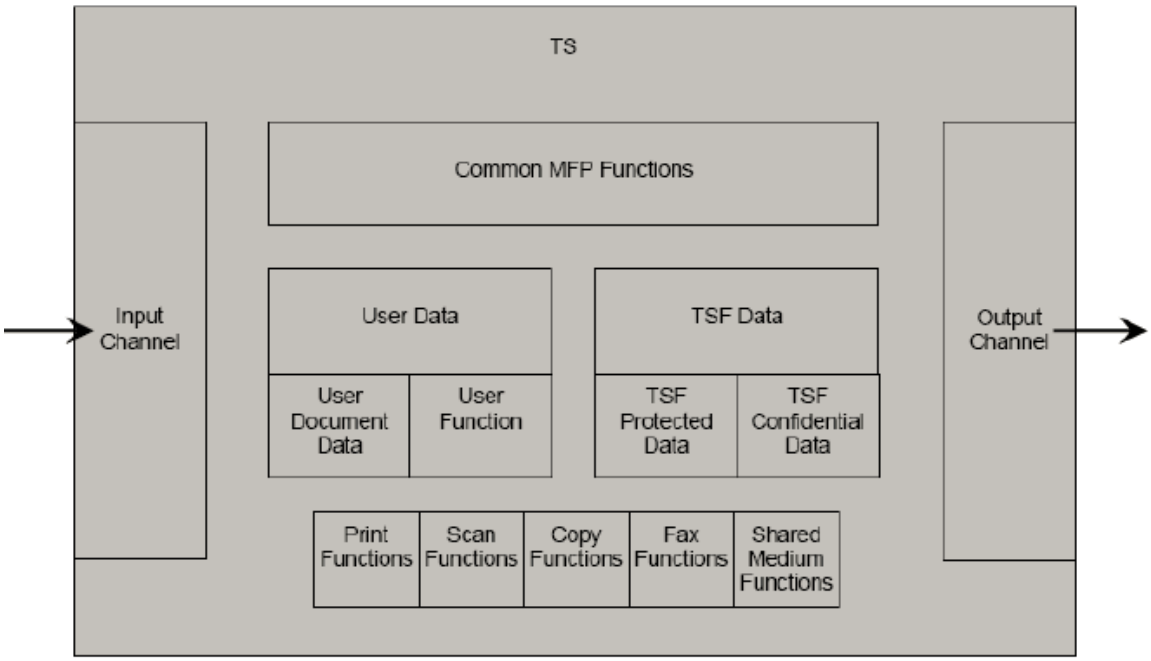

Figure 1, TOE model

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 SFP 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 subsystem (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.

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, formats it for display in the remote browser session, and forwards the information to the remote browser session. It also processes input received from the remote browser session. When configuration changes are made, the updated information is sent to the Object Store subsystem to be saved and acted on.

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 CS620 Series User's Guide
- Lexmark CS920, CS921, CS922, CS923, CS924, CS927 User's Guide
- Lexmark MS620 Series User's Guide
- Lexmark MS820 Series User's Guide

7 IT Product Testing

7.1 Developer Testing

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 all firmware and all printer models.

7.2 Evaluator Testing

The evaluator's independent tests were chosen to complement the developer's manual tests in order to complement the cover of the security functional behavior of the TSFIs and SFRs. The evaluator repeated developer's test cases and performed individual and penetration test cases. 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: CS923, CS622, MS622, and MS822
- 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
- IP Network

The tests were run manually from the SFP'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.

7.3 Penetration Testing

The following types of vulnerability tests were performed:

- Port scan
- Vulnerability scan
- PNG fuzzing
- Communication protocol compliance
- IKE/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 SFP 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 17, 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 24 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 SFP. The SFP 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 SFP:

- A LAN for network connectivity. The TOE supports IPv4 and IPv6.

- IT systems that submit print jobs to the SFP via the network using standard print protocols.

- 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 identification and authentication mechanisms used.

- Card reader and cards to support Smart Card authentication using Common Access Card (CAC), Personal Identity Verification (PIV) cards or Secret Internet Protocol Router Network (SIPRNet) cards. This component is optional depending on the type(s) of identification and authentication mechanisms used. The supported card readers are:

a. Identiv uTrust 2700 F Contact Smart Card Reader & Identiv uTrust 2700 R Contact Smart Card Reader

b. Omnikey 3121 SmartCard Reader

c. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the Omnikey 3121 (example Omnikey 3021)

d. SCM SCR 331

e. 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 SFPs that perform document processing functions.
  - Option card for downloadable emulators.
- Other I&A mechanisms than Internal Accounts, LDAP+GSSAPI on a per-user basis, and Smart Card authentication.
- Other eSF, Java applications, than
  - Smart Card Authentication,
  - Smart Card Authentication Client,
  - Display Customization
  - Secure Email
  - Secure Held Jobs

  - PIV Smart Card Driver (if PIV cards are used)
  - CAC Smart Card Driver (if CAC cards are used)", and
  - SIPRNet Smart Card Driver (if SIPRNet cards are used)
- 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
Systematic flaw remediation	ALC_FLR.3	PASS
Development	ADV	PASS
Security Architecture description	ADV_ARC.1	PASS
Functional specification with complete summary	ADV_FSP.3	PASS
Architectural 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 - Sample	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 Organization for Standardization
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
NTP	Network Time Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PJL	Printer Job Language
PP	Protection Profile
SFP	Single-Function Printer
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 5, April 2017, CCMB-2017-04-001
[CCp2]	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002
[CCp3]	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
[ST]	Lexmark CS622, CS921, CS923, MS622, MS822, and MS826 Single Function Printers Security Target, Lexmark International, Inc., 2018-11-08, document version 1.9
[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
1.21.1	2018-03-09	Original version
1.21.2	2018-03-09	None
1.21.3	2018-05-24	None
1.21.4	2018-09-13	None
1.21.5	2018-11-19	None
1.22	2019-02-01	None
1.22.1	2019-03-08	None
1.22.2	2019-05-02	None
1.22.3	2019-05-20	None

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	
SN-18	2.0	Highlighted Requirements on the Security Target	