Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Lexmark MX522, MX622h, MX721h, MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923, CX924, M C550SRF, M C550FG w/firmware 073.239 and Lexmark Secure Element (P/N 57X0185)

14 January 2021

521-EWA-2020

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Lexmark MX522, MX622h, MX721h, MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923, CX924, M C550SRF, M C550FG w/firmware 073.239 and Lexmark Secure Element (P/N 57X0185), hereafter referred to as the Target of Evaluation, or TOE, from Lexmark International, Inc., was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 January 2021 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Lexmark MX522, MX622h, MX721h, MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923, CX924, M C550SRF, M C550FG w/firmware 073.239 and Lexmark Secure Element (P/N 57X0185)
Developer	Lexmark International, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

Protection Profile for Hardcopy Devices, v1.0, Sept 2015

Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017

1.2 TOE DESCRIPTION

The TOEs are multi-functional printer systems with scanning, fax, and networked capabilities. Their capabilities extend to walk-up scanning and copying, scanning to fax, scanning to email, and servicing print jobs through the network. The MFPs feature an integrated touch-sensitive operator panel.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

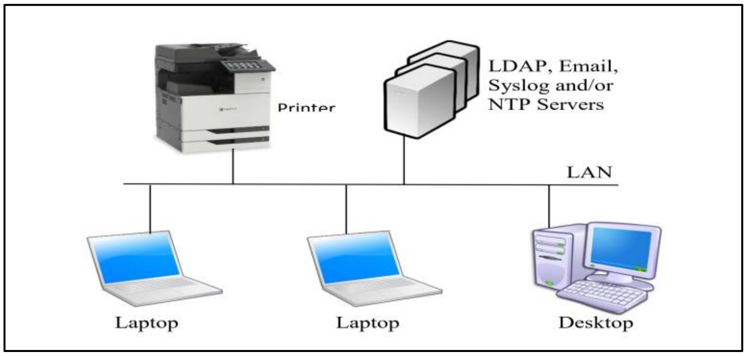

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CAVP and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Cryptographic Algorithm	Certificate Number
AES (CBC)	C1753, C1758, C1754, C1759, C1752, C1757
DRBG (CTR_DRBG(AES))	C1758, C1759, C1757
HMAC	C1753, C1758, C1754, C1759 C1752, C1757
RSA	C1758, C1759, C1757
SHA	C1753, C1758, C1754, C1759 C1752, C1757
CVL (IKEv1, IKEv2)	C1758, C1759, C1757

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
- The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
- TOE Administrators are trusted to administer the TOE according to site security policies.
- Authorized Users are trained to use the TOE according to site security policies.

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

The following functionality is supported in the product but is not included in the evaluation:

- Common Access Card (CAC) and Secret Internet Protocol Router Network (SIPRNet) cards,
- Identiv uTrust 2700 R Contact Smart Card Reader,
- Omnikey 3121 SmartCard Reader,
- Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the Omnikey 3121 (example Omnikey 3021),
- SCM SCR 331, and
- SCM SCR 3310v2.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises Lexmark MX522, MX622h, MX721h, MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923, and CX924 and Ricoh M C550SRF and M C550FG Multi-Function Printers with Hard Drives with firmware version xxxxx.073.239 with Lexmark Secure Element (P/N 57X0185). The build type of the firmware version identifier (xxxxx as shown above) is one of the following:

- MXTGM: MX522, MX622h
- MXTGW: MX721h, MX722h, MX822, MX826
- CXTZJ: CX622h, CX625h
- CXTAT: CX725h
- CXTPP: CX820, CX825, CX860, M C550SRF, M C550FG
- CXTMH: CX920, CX921, CX922, CX923, CX924

The first letter in the identifier is C for color printers or M for mono printers. The next two letters are always XT, signifying multi-function devices. Note that the Ricoh models are Lexmark OEM models using the same firmware as the Lexmark CX860.

The evaluated configuration requires support from the operating environment for the following:

- SYSLOG server
- LDAP server
- NTP server
- Email server
- Identiv uTrust 2700 F Contact Smart Card Reader
- Telephone line

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Lexmark Common Criteria Installation Supplement and Administrator Guide, September 2020

b) Lexmark Embedded Web Server – Security Administrator's Guide, April 2018

c) Lexmark CX421, CX522, CX622, CX625, MC2325, MC2425, MC2535, MC2640, XC2235, XC4240 MFPs User's Guide, December 2018

d) Lexmark CX725, CX725R, CX727 MPFs User's Guide, June 2019

e) Lexmark CX820, CX827 User's Guide, October 2017

f) Lexmark CX825, CX860 User's Guide, February 2018

g) Lexmark CX920, CX921, CX922, CX923, CX924, CX927 User's Guide, September 2018

h) Lexmark MB2442, MB2546, MX421, MX521, MX522, XM1242, XM1246 MFPs User's Guide, September 2018

i) Lexmark MB2650, MX622, XM3250 MFPs User's Guide, February 2020

j) Lexmark MB2770, MX721, MX722, MX725, XM5365, XM5370 MFPs User's Guide, December 2018

k) Lexmark MX822, MX826, XM7355, XM7370 MFPs User's Guide, March 2020

l) Embedded Web Server Administrator's Guide, April 2020

m) M C550SRF/M C550FG User’s Guide, April 2020

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP;

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations were present and used by the TOE;

c. User Data Persistence after Restart of TOE: The evaluator verified that a print job persists across a power outage, prints correctly and the U.ADMIN login does not persist; and

d. Faxing a Postscript File: The evaluator verified that the TOE will not start a new job created by a Postscript File.

6.3.1 FUNCTIONAL TEST RESULTS

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1 PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on 11/13/2020 and included the following search terms:

- Multi-Function Printers, Lexmark MX522, MX622h, MX721h, MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923, and CX924 and Ricoh M C550SRF and M C550FG; Lexmark MFP; firmware MXTGM.073.239; MXTGW.073.239; CXTZJ.073.239; CXTAT.073.239; CXTPP.073.239; and CXTMH.073.239, Lexmark Airprint; Lexmark Thinprint; Google Cloudprint; SIPR Smartcard 1.3.7; CAC Smartcard 1.3.7; Secure E-mail 2.1.11; Scan Center 1.5.20; PIV Smartcard 1.3.10; Card Copy 4.3.30; Scan Center - Printer 1.5.2; Scan Center – Network Folders 1.5.9; and Scan Center - Fax 1.5.3.

Vulnerability searches were conducted using the following sources:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases)
- Lexmark Support
- Google

The independent penetration testing did not uncover any residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

- It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Lexmark and Ricoh Multi-Function Printers with Hard Drives Security Target, Version 1.9, December 16, 2020.
Evaluation Technical Report for the Common Criteria evaluation of Lexmark MX522, MX622h, MX721h,MX722h, MX822, MX826, CX622h, CX625h, CX725h, CX820, CX825, CX860, CX920, CX921, CX922, CX923,and CX924 and Ricoh M C550SRF and M C550FG Multi-Function Printers with Hard Drives with firmware version xxxxx.073.239 with Lexmark Secure Element (P/N 57X0185), Version 1.5, January 14, 2021.
Assurance Activity Report Lexmark and Ricoh Multi-Function Printers with Hard Drive, Version 0.13, January 14, 2021.