Communications Security Establishment

Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

collaborative Protection Profile for Hardcopy Devices Version 1.0E

10 September 2024

628-LSS

V1.0

Canada

FOREWORD

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

The Protection Profile identified in this certification report has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (CCCS). This certification report applies only to the identified version and release of the Protection Profile. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

If your organization has identified a requirement for this certification report and would like more detailed information, please contact:

Canadian Centre for Cyber Security
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 Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL 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.

This certification report is posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF TABLES

EXECUTIVE SUMMARY

This report documents the results of the evaluation of the **collaborative Protection Profile for Hardcopy Devices Version 1.0E** . It presents a summary of the protection profile and the evaluation results.

To promote thoroughness and efficiency, the evaluation of the protection profile was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the **Lexmark MX532, MX632, CX532, and CX635 Multi-Function Printers with Hard Drive and with Firmware Version 222.037** (hereafter referred to as the 628-LSS or TOE).

The evaluation was performed by **Lightship Security** and was completed **10 September 2024.** An additional evaluation of the PP was performed by the CCTL to confirm that it meets the claimed APE assurance requirements.

The evaluations determined that the protection profile is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Canadian Centre for Cyber Security, as the Certification Body, found that the evaluations demonstrated that the protection profile meets the requirements of the APE components. The conclusions of the testing laboratory in the Assurance Activity Report are consistent with the evidence produced.

1 IDENTIFICATION

The Protection Profile (PP) is identified as follows:

Table 1: PP Identification

PP Name and Version	**collaborative Protection Profile for Hardcopy Devices Version 1.0E**
CCTL	**Lightship Security**

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.

1.2 PP DESCRIPTION

This collaborative Protection Profile (cPP) is designed to evaluate hardcopy device (HCD) job functions such as converting hardcopy documents into digital form (scanning), converting digital documents into hardcopy form (printing), duplicating hardcopy documents (copying), or transmitting documents over a Public Switched Telephone Network (PSTN) connection (PSTN faxing). Hardcopy documents typically take the form of paper but can take other forms (e.g. transparencies).

For this cPP, a conforming HCD must support at least one of the job functions printing, scanning, or copying and must support the functions network communications and administration.

2 SECRUITY PROBLEM DEFINITION

2.1 ASSUMPTIONS

The specific conditions listed here are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2: Assumptions

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

2.2 THREATS

TOEs conforming to the PP counter the following threats.

Table 3: Threats

Name	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component.
T.TSF_FAILURE	A malfunction of the TSF may compromise the device security status if the TOE is permitted to operate
T.UNAUTHORIZED_UPDATE	An attacker may install unauthorized firmware/software on the TOE to modify the Device security status.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

Name	Definition
T.WEAK_CRYPTO	An attacker may exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes to access (read, modify, or delete) TSF and User data.

2.3 ORGANIZATIONAL SECURITY POLICIES

The following organizational security polices are expected to be in affect for the TOEs operational environment.

Table 4: Organizational Security Policies

Name	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be stored within the TOE as well as protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.
P.WIPE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
P.ROT_INTEGRITY	The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters.

3 SECURITY OBJECTIVES

The following table contains security objectives for the TOE.

Table 5: TOE Security Objectives

Name	Definition
O.USER_I&A	The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.
O.ACCESS_CONTROL	The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.
O.USER_AUTHORIZATION	The TOE shall perform authorization of Users in accordance with security policies.
O.ADMIN_ROLES	The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.
O.UPDATE_VERIFICATION	The TOE shall provide mechanisms to verify the authenticity of firmware/software updates.
O.TSF_SELF_TEST	The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.
O.COMMS_PROTECTION	The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing.
O.AUDIT	The TOE shall generate audit data and store it internally as well as be capable of sending it to a trusted External IT Entity.
O.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data in Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.
O.KEY_MATERIAL	The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material.
O.FAX_NET_SEPARATION (conditionally mandatory)	If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function.
O.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Nonvolatile Storage Devices.

Name	Definition
O.WIPE_DATA (optional)	The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.
O.AUTH_FAILURES (conditionally mandatory)	The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
O.FW_INTEGRITY	The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.
O.STRONG_CRYPTO	The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

The following table contains security objectives for the Operational Environment.

Table 6: Environmental Security Objectives

Name	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

4 SECURITY REQUIREMENTS

4.1 SECURITY FUNCTIONAL REQUIREMENTS

The protection profile is comprised of the “base” requirements and additional requirements that are optional, selection based and conditionally mandatory.

Table 7: “Base” Security Functional Requirements

Class	Component	Verified by
FAU: Security Audit	FAU_GEN.1 Audit data generation	628-LSS
	FAU_GEN.2 User identity association	628-LSS
	FAU_SAR.1 Audit review	628-LSS
	FAU_SAR.2 Restricted Audit Review	628-LSS
	FAU_STG.1 Protected audit trail storage	628-LSS
	FAU_STG.4 Prevention of audit data loss	628-LSS
	FAU_STG_EXT.1 Extended: External Audit Trail Storage	628-LSS
FCS: Cryptographic Support	FCS_CKM.1/AKG Cryptographic Key Generation (Asymmetric Keys)	628-LSS
	FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)	628-LSS
	FCS_CKM.2 Cryptographic Key Establishment	628-LSS
	FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction	628-LSS
	FCS_CKM.4 Cryptographic key destruction	628-LSS
	FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)	628-LSS
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	628-LSS
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	628-LSS
	FCS_RBG_EXT.1 Random Bit Generation	628-LSS
User Data Protection	FDP_ACC.1 Subset access control	628-LSS
	FDP_ACF.1 Security attribute-based access control	628-LSS
FIA: Identification and Authentication	FIA_ATD.1 User attribute definition	628-LSS
	FIA_PMG_EXT.1 Extended: Password Management	628-LSS

Class	Component	Verified by
	FIA_UAU.1 Timing of authentication	628-LSS
	FIA_UAU.7 Protected authentication feedback	628-LSS
	FIA_UID.1 Timing of identification	628-LSS
	FIA_USB.1 User-subject binding	628-LSS
FMT: Security Management	FMT_MOF.1 Management of security functions behavior	628-LSS
	FMT_MSA.1 Management of security attributes	628-LSS
	FMT_MSA.3 Static attribute initialization	628-LSS
	FMT_MTD.1 Management of TSF data	628-LSS
	FMT_SMF.1 Specification of Management Functions	628-LSS
	FMT_SMR.1 Security roles	628-LSS
FPR: Privacy	There are no class FPR requirements	
FPT: Protection of the TSF	FPT_SBT_EXT.1 Extended: Secure Boot	628-LSS
	FPT_SKP_EXT.1 Extended: Protection of TSF Data	628-LSS
	FPT_STM.1 Reliable time stamps	628-LSS
	FPT_TST_EXT.1 Extended: TSF testing	628-LSS
	FPT_TUD_EXT.1 Extended: Trusted Update	628-LSS
FRU: Resource Utilization	There are no class FRU requirements	
FTA: TOE Access	FTA_SSL.3 TSF-initiated termination	628-LSS
FTP: Trusted Path/Channels	FTP_ITC.1 Inter-TSF trusted channel	628-LSS
	FTP_TRP.1/Admin Trusted path (for Administrators)	628-LSS

Table 8: “Optional” Security Functional Requirements

Class	Component	Verified by
FDP: User Data Protection	FDP_UDU_EXT.1 Document Unavailability	628-LSS

Class	Component	Verified by
FPT: Protection of the TSF	FPT_WIPE_EXT.1 Data Wiping	628-LSS
FCS: Cryptographic Support	FCS_DTLSC_EXT.2 DTLS Client Support for Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication	PP Evaluation
	FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication	PP Evaluation
	FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication	PP Evaluation

Table 9: “Selection-Based” Security Functional Requirements

Class	Component	Verified by
FCS: Cryptographic Support	FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)	628-LSS
	FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)	PP Evaluation
	FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)	PP Evaluation
	FCS_COP.1/KeyTransport Cryptographic operation (Key Transport)	PP Evaluation
	FCS_SMC_EXT.1 Extended: Submask Combining	PP Evaluation
	FCS_IPSEC_EXT.1 Extended: IPsec selected	628-LSS
	FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication	PP Evaluation
	FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication	PP Evaluation
	FCS_SSHC_EXT.1 SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1 SSH Server Protocol	PP Evaluation
	FCS_HTTPS_EXT.1 Extended: HTTPS selected	PP Evaluation
	FCS_COP.1/Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)	628-LSS
	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	628-LSS
	FCS_DTLSC_EXT.1 DTLS Client Protocol Without Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.1 DTLS Server Protocol Without Mutual Authentication	PP Evaluation

Class	Component	Verified by
	FCS_PCC_EXT.1 Extended: Cryptographic Password Construct and Conditioning	PP Evaluation
	FCS_KDF_EXT Extended: Cryptographic Key Derivation	PP Evaluation
	FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication)	PP Evaluation
	FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1 X.509 Certificate Validation	628-LSS
	FIA_X509_EXT.2 X.509 Certificate Authentication	628-LSS
	FIA_X509_EXT.3 X.509 Certificate Requests	628-LSS

Table 10: “Conditionally Mandatory” Security Functional Requirements

Class	Component	Verified by
FPT: Protection of the TSF	FPT_KYP_EXT.1 Extended: Protection of Key and Key Material	628-LSS
FCS: Cryptographic Support	FCS_KYC_EXT.1 Extended: Key Chaining	628-LSS
FDP: User Data Protection	FDP_DSK_EXT.1 Extended: Protection of Data on Disk	628-LSS
	FDP_FXS_EXT.1 Extended: Fax separation	628-LSS
FTP: Trusted Path/Channels	FTP_TRP.1/NonAdmin Trusted path (for Non-administrators)	628-LSS
FIA: Identification and Authentication	FIA_AFL.1 Authentication failure handling	628-LSS

4.2 SECURITY ASSURANCE REQUIREMENTS

The protection profile contains the following assurance requirements:

Table 11: Security Assurance Requirements

Class	Component	Verified by
ASE: Security Target	Conformance Claims (ASE_CCL.1)	628-LSS
	Extended components definition (ASE_ECD.1)	628-LSS
	ST introduction (ASE_INT.1)	628-LSS
	Security objectives for the operational environment (ASE_OBJ.1)	628-LSS
	Stated security requirements (ASE_REQ.1)	628-LSS
	Security Problem Definition (ASE_SPD.1)	628-LSS
	TOE summary specification (ASE_TSS.1)	628-LSS
ADV: Development	Basic functional specification (ADV_FSP.1)	628-LSS
AGD: Guidance Documents	Operational user guidance (AGD_OPE.1)	628-LSS
ALC: Life Cycle Support	Labeling of the TOE (ALC_CMC.1)	628-LSS
	TOE CM coverage (ALC_CMS.1)	628-LSS
ATE: Tests	Independent testing – conformance (ATE_IND.1)	628-LSS
AVA: Vulnerability Assessment	Vulnerability survey (AVA_VAN.1)	628-LSS

5 RESULTS OF THE EVALUATION

Note that for APE elements and work units that are identical to ASE elements and work units, the testing laboratory performed the APE work units concurrent to the ASE work units. In addition, the testing laboratory performed a separate APE evaluation of the protection profile that was independent of the product evaluation.

Table 12: Evaluation Results

APE Requirement	Evaluation Verdict	Verified by
APE_CCL.1	Pass	628-LSS
APE_ECD.1	Pass	628-LSS
APE_INT.1	Pass	628-LSS
APE_OBJ.1	Pass	628-LSS
APE_REQ.1	Pass	628-LSS
APE_SPD.1	Pass	628-LSS

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
CCTL	Common Criteria Testing Laboratory
cPP	Collaborative Protection Profile
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HCD	Hardcopy Device
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
PTSN	Public Switched Telephone Network
RoT	Root of Trust
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

6.2 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.
APE Protection Profile Evaluation collaborative Protection Profile for Hardcopy Devices v1.0 Evaluation Technical Report, Version 1.1, July 5, 2024.
Lexmark MX532, MX632, CX532, and CX635 Multi-Function Printers with Hard Drive and with Firmware Version 222.037 Security Target, Version 1.20, September 10, 2024.
Lexmark MX532, MX632, CX532, and CX635 Multi-Function Printers with Hard Drive and with Firmware Version 222.037, Evaluation Technical Report Version, 1.7, September 10, 2024.
Lexmark MX532, MX632, CX532, and CX635 Multi-Function Printers with Hard Drive and with Firmware Version 222.037, Assurance Activity Report, Version 1.10, September 10, 2024.