National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs).

Report Number: CCEVS-VR-07-0059

Dated: 21 September 2007

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers
Dianne Hale

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs) at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on June 29, 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.3, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs).

The TOE is comprised of the MFP System Firmware. It includes security functionality as it applies to the features listed below:

Fax Communications Control
The Fax Communications Control 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 analog fax function. Control of the fax functionality is incorporated directly into the TOE's firmware. There is no mechanism by which telnet, FTP, or other network protocols can be sent or received over the analog fax line. Reference Section 3.1.1.1 for additional details.

User Authentication
The TOE's display interface allows access to the print-from USB operation and the following types of scan-based operations to touch screen users: scan-to-fax, scan-to-copy, scan-to-USB, and scan-to-email. Each of these operations is restricted with the User Authentication function, which requires the touch screen user's credentials to be submitted and validated before the TOE gives the touch screen user access to the operation.
Note that no identification or authentication is performed for network print users or inbound fax users. Reference Section 3.1.1.2 for additional details.

Device Configuration Protection
The configurable settings that control the behaviour of the MFP can only be modified after authentication with the TOE's administrative credentials. In addition, management of the MFP occurs primarily via remote access utilizing HTTPS. These sessions provide protection against disclosure and modification via SSL v2 and v3 and TLS v1. Reference Section 3.1.1.3 for additional details.

TSF Self Protection
The MFP protects itself by ensuring that security functions may not be bypassed by activities within the TSC and by implementing security domains that protect it from interference and tampering by untrusted subjects within the TSC. Reference Section 3.1.1.4 for additional details.
.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS’ Validated Products List. Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifier

Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs).	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs).
Protection Profile	N/A
Security Target	Lexmark X642e and X644e Multifunction Printer (MFP) Security Target, Document No. SV-0606-003(1.9), dated August 31, 2007
Evaluation Technical Report	Evaluation Technical Report for the Lexmark X642e and X644e Multifunction Printer (MFP), Document No. F2-0807-004, dated September 5, 2007.
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.3 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on January 26, 2006.
Version of CEM	CEM Version 2.3 and all applicable NIAP and International Interpretations effective on January 26, 2006.
Sponsor	Lexmark, Inc. 740 New Circle Road NW Lexington, KY 40511
Developer	Lexmark, Inc. 740 New Circle Road NW

Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs).	
	Lexington, KY 40511
Evaluator(s)	**COACT Incorporated** Bob Roland Greg Beaver Christa Lanzisera Tom Benkart
Validator(s)	**NIAP CCEVS** Jerome F. Myers Diane Hale

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 TOE Description

The Lexmark X642e (firmware revision LC2.MB.P237) and X644e (firmware revision LC2.MC.P239b) Multifunction Printers (MFPs) consist of the following components of the MFP:

- Fax Communications Control
- User Authentication
- Device Configuration Protection
- TSF Self Protection

These components are explained in the subsections below.

3.1.1.1 Fax Communications Control

The Fax Communications Control 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 analog 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 is the document that was submitted for faxing.
The Fax Communications Control security function is inherent in the design of the system, and is not explicitly activated. Control of the fax functionality is incorporated directly into the TOE's firmware. The fax chip that sends and receives data over the phone line is directly controlled by the TOE firmware. The modem chip is in a mode that's more restrictive than Class 1 mode, and relies on the TOE firmware for composition and transmission of fax data. The TOE firmware explicitly disallows the transmission of frames in data mode and allows for the sending and

receiving of facsimile jobs, only. There is no mechanism by which telnet, FTP, or other network protocols can be sent or received over the analog fax line.

3.1.1.2 User Authentication

The TOE's display interface allows access to the following types of scan-based operations to touch screen users: scan-to-fax, scan-to-copy, scan-to-USB, and scan-to-email. The TOE's display interface also allows access to the print-from-USB operation to touch screen users. Each of these operations is restricted with the User Authentication function, which requires the touch screen user's credentials to be submitted and validated before the TOE gives the touch screen user access to the operation. The authentication is performed against a set of touch screen user accounts that are maintained by the TOE. The TOE touch screen user account passwords are configurable and are a minimum of six characters in length.

If for any reason the User ID and Password provided by the touch screen user do not match a set of credentials in the list of touch screen user accounts, access is denied and the touch screen user is prompted again.

After three successive failed attempts at authentication, the touch screen user is notified with the GUI represented in the following figure. The system does not lock out the touch screen user account.

Note that no identification or authentication is performed for network print users or inbound fax users. These roles may transmit (via the local area network or fax line respectively) data to be printed on the embedded printer, and have no access to any other security-relevant functions.

3.1.1.3 Device Configuration Protection

The TOE's System Administrator password is configurable and is a minimum of eight characters in length. The administrative account cannot be deleted, or disabled. There are no means to add any system administrator authority to touch screen user accounts.

When a remote session is established to the MFP via HTTPS, the user has access to a device status page. If access is attempted to any of the configuration menus, the user is prompted to provide the System Administrator password. If an invalid Password is specified, access is denied and the user is prompted again.

System Administrators can perform such tasks as creating user accounts and updating user passwords. The MFP device includes parameters that can be configured by an administrator. The Device Configuration Protection function restricts the ability to configure those parameters by requiring authentication against the TOE's administrative account.

The configurable settings that control the behaviour of the MFP related to scanning, email, authentication, and all other major functions can only be modified after authentication with the TOE's administrative credentials.

Management of the MFP occurs via remote access utilizing HTTPS. These sessions provide protection against disclosure and modification via SSL v2 and v3 and TLS v1.

3.1.1.4 TSF Self Protection

The MFP protects itself by ensuring that security functions may not be bypassed by activities within the TSC and by implementing security domains that protect it from interference and tampering by untrusted subjects within the TSC.

The MFP maintains separate memory spaces for its various processes, and uses well-defined interfaces for interprocess communication to control interactions between the processes. Remote login to a command prompt and the remote execution of MFP services is not allowed. The TSF Self Protection function is inherent in the architecture of the system, and does not rely on external interfaces or explicit activation.

4 Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

A.NOEVIL System Administrators are not evil, follow the Lexmark MFP Administrative Guidance before exercising security management functions related to the system, and do not attempt to attack or subvert the TOE and its policy. System Administrators are responsible for managing the TOE and the security of the information it contains.

A.LOCATE The processing resources of the TOE will be located within non-hostile facilities that will prevent unauthorized physical access by hostile individuals who could compromise the TSF.

5 Threats

The threats identified in the following table sections are addressed by the TOE and/or Operating Environment.The following threats are addressed by the TOE and IT environment, respectively.

T.ACCESS An unauthorized individual may attempt to gain access to the TOE functions and to TOE resources through either malicious or accidental means.

T.FAXLINE A hostile entity may attempt to gain unauthorized access through a phone connection to TOE resources, or TOE connected networks to retrieve data of value.

T.NOAUTH An authorized user may attempt to gain unauthorized access to TOE security functions

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. This evaluation does not verify all claims made in the product's end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5 and 6 respectively). Section 7.1 of this report also provides a list of functionality excluded from the evaluation.
2. This evaluation only covers the evaluated configuration of the specific versions identified in this document, and not any later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious." The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. These products make use of internet protocols for remote communication with the devices (TLSv1.0, SSLv2, and SSLv3). These protocols, while used during testing, were

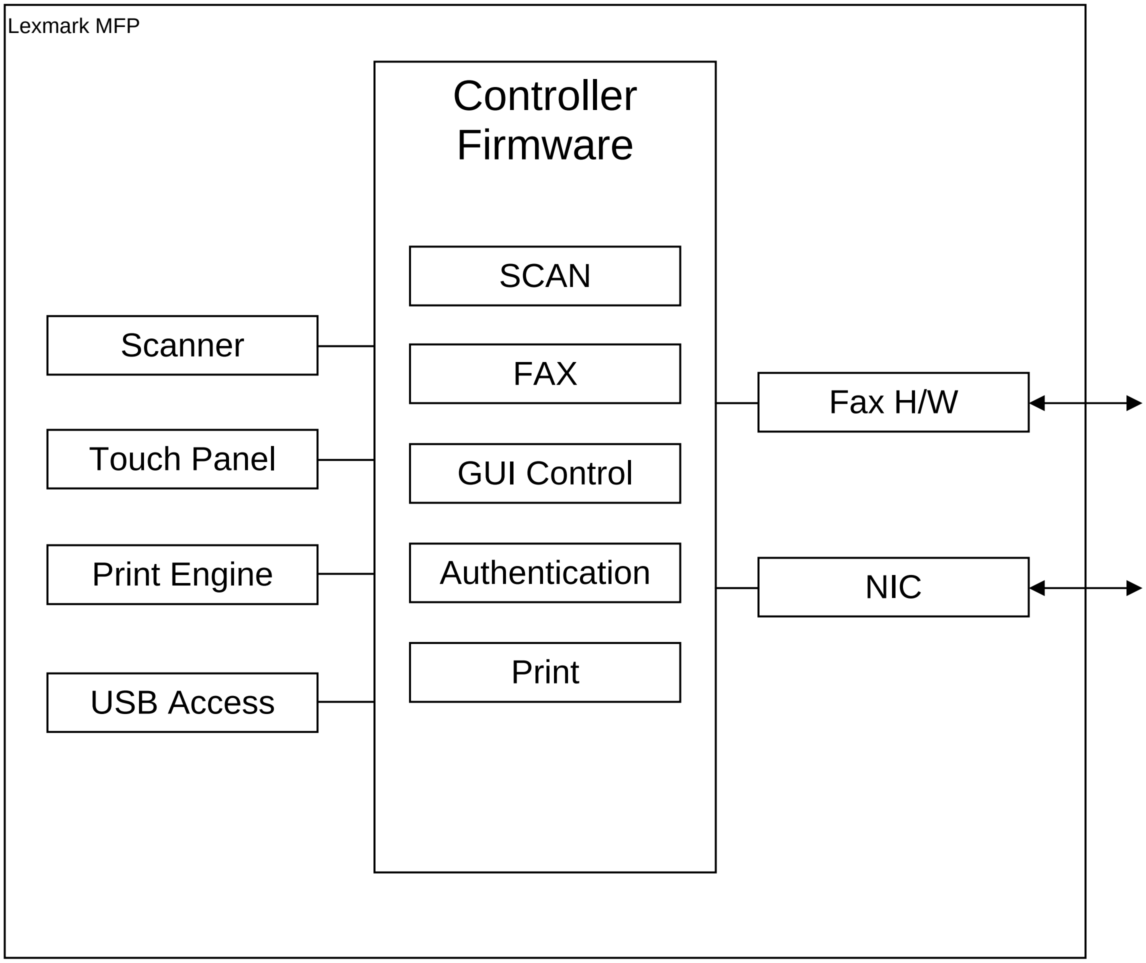
not confirmed to operate completely in accordance with the appropriate RFC by the CCTL. That is, not all optional parameters specified in the RFC were tested; therefore the protocols remain self-certified by the vendor.

The ST provides additional information on the assumptions made and the threats countered.

7 Architecture Information

The Lexmark MFP is a multi-functional printer system with scanning, fax, and networked capabilities. Its capabilities extend to walk-up scanning and copying, scanning to fax, scanning to email, and servicing print jobs through the network. The MFP also enables users to insert a USB Drive, which can be used as the source for print operations or the destination for scan operations. The MFP includes print, fax and scan functionality with an integrated touch-sensitive operator panel. The TOE is the complete MFP and implements the TOE Security Functions of Fax Communications Control, User Authentication, Device Configuration Protection, and TSF Self Protection. The figure below illustrates the physical boundaries and its interactions:

Figure 1 - Lexmark MFP Product Description



7.1 Evaluated Configuration

Lexmark X642e and X44e MFPs Evaluated Configuration.

The evaluated configuration will be as detailed below:

A) Internal User Authentication is selected for the authentication mode.

B) All scan and print operations accessible via the touch screen operator panel require users to successfully identify and authenticate before proceeding.

C) HTTPS is enabled; HTTP is disabled.

D) All security-relevant system administrator functions other than Hard Disk Sanitization occur through a browser using HTTPS. Access to the device configuration menus other than Hard Disk Sanitization through the Touch Screen is disabled.

E) The Advanced Password is configured for all system administration functions. Access to specific configuration pages available through HTTPS requires knowledge of the Advanced Password to gain access. Configuration of the specific pages is detailed in the following table.

Table 2 - System Administration Web Page Access

Web Page	Description	Controlled Access?
Device Status	Displays device information including Tray size and capacity, toner status, and output bin status. Nothing on the TOE can be configured from this page.	No
Scan Profile	Allows the administrator to create a scan profile on the TOE that enables a user to scan a document back to their local computer.	Yes
Reports	Contains device reports.	Yes
Links & Index	Contains links to public Lexmark.com websites that allow operators to get technical support, order supplies, and get other general interest information. This page also contains an index of links to all the configuration pages contained under the configuration menu. All of the index links use the same security settings as the configuration menu	Yes
Applications	Displays any extra Lexmark applications installed on the TOE. In the evaluated configuration, there are no applications installed and this page is basically empty.	Yes
Order Supplies	Direct link to the Lexmark.com homepage.	No
Configuration	Provides links to all the configuration submenus.	No, but access to all of the configuration submenus is restricted

F) FTP server functionality is disabled.

G) The NetWare protocol is disabled.
H) The AppleTalk protocol is disabled.
I) The DLC protocol is disabled.
J) The MVP management protocol is disabled.
K) SNMP is disabled.

Functionality Not Included in the Evaluation
The following functionality is present in the MFPs but was not included in the evaluation:
A) Integration with external authentication servers
B) Restricted server list
C) Embedded solutions
D) 802.1x authentication
E) Confidential print
F) IPSec support
G) Integration with external time servers
H) Ability to update the firmware
I) Importing configuration files
J) Sending email alerts
K) Touch Screen Lock

8 Product Delivery

Lexmark's Multifunction Printer (MFP) products are composed of a single unit scanner. There is one set of controller firmware which resides in the TOE. The units are manufactured by Lexmark International and delivered via sea and land to their final destinations. A set of commercial shipping companies are used to ship, warehouse, and ultimately deliver the products.

During the shipping, warehousing, and delivery processes the product is secured by its physical packaging: each unit is stored individually in cardboard packaging, and the products are shipped on pallets that are shrink-wrapped for protection against environmental exposure as well as protection from tampering or theft.

A Lexmark service representative visits the customer site and configures the MFP in a manner consistent with the evaluated configuration. This ensures that the security settings are appropriately configured, and the appropriate TOE software version is in use.

In addition to the physical packaging, the TOE is protected by its own design. At the customer's request, a Lexmark representative can update the TOE by applying software update packages authorized by Lexmark. During such a software update, the update package is transmitted to the TOE and inspected by the TOE. The software update must be of the appropriate proprietary format, and the package must include digital signatures provided by Lexmark. If the software update does not meet these criteria, it is discarded by the TOE. This mechanism provides protection against malicious or unauthorized code being placed onto the product, should physical access be obtained during the shipping process.

Model Name	Description	Evaluated
Lexmark X642e Lexmark X644e	Network Setup Sheet (P/N22G0472)	Yes

Model Name	Description	Evaluated
	Local Setup Sheet (P/N22G0476)	Yes
	Safety Information Sheet (P/N20G0383)	No
	Safety Stability Sheet (P/N20G0629)	No
	Software and Documentation CD (P/N22G0460)	Yes
	Warranty Sheet/Book (1991)	No
	WEEE Booklet (P/N10B4407)	No
	Supplies Return Program Flyer (P/N12A7718)	No

Contents of the Software and Documentation CD

A) User's Guide
B) Menus and Messages Guide
C) Help pages
D) Drivers and Utilities

9 IT Product Testing

Testing was performed between April 4 through April 6 2007 at the Lexmark facilities in Lexington, Kentucky. COACT employees performed the tests.

9.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

The following hardware components are required for the TOE functional testing. Note: this test configuration is used for both the repeated developer tests and the independent functional tests.

A) MFP (TOE): X644e MFP (IP Address 157.184.87.132)

B) PC 1 – Used for administrative access

C) PC 2 – Used to Sniff TOE administrative communication

D) Hub

The following software components are required for the TOE functional testing:

A) MFP (TOE): X644e MFP (IP Address 157.184.87.132)

   1. No additional software required

B) PC 1 – Used for administrative access

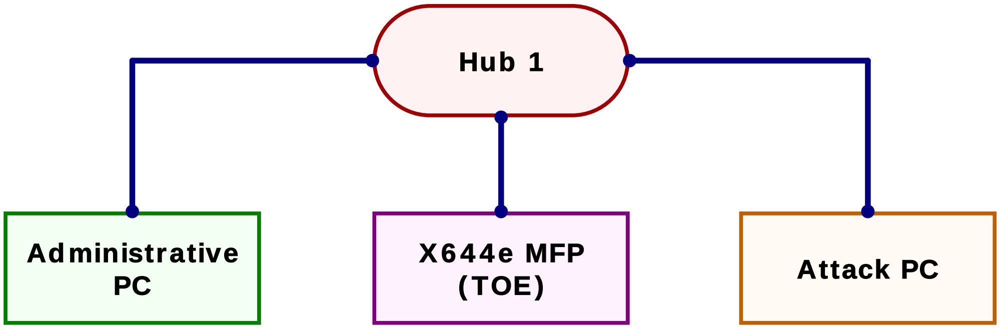
   1. Opera Web browser

C) PC 2 – Used to Sniff TOE administrative communication

   1. Wireshark Traffic Sniffer
   2. Opera Web browser

The following figure graphically displays the test configuration used for functional testing.

Test Configuration/Setup



9.2 Functional Test Results

The repeated developer test suite includes seven of the fifteen developer functional tests. This figure is forty-six percent (46%) of the complete developer test suite. This figure falls well with the Common Criteria recommended sample of twenty percent (20%). Additionally, each of the Security Function and developer tested TSFI are included in the CCTL test suite. Results are found in the Lexmark No HDD Test Report, Document No. F2-0807-005, dated September 5, 2007.

9.3 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. For example, specific TSFI behaviors were identified while performing the ADV work units, and tests have been developed to test specific behaviors. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

9.4 Evaluator Penetration Tests

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

A) http://www.osvdb.org/
B) www.sans.org
C) www.cert.org

D) www.isc2.org
E) http://nvd.nist.gov/

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicting that the vulnerability is non-exploitable in the intended environment of the TOE.
While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.
The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

9.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

10 RESULTS OF THE EVALUATION

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the MFP for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, Lexmark X642e and X644e Multifunction Printer (MFP) Penetration Test Report, Document No. F2-0807-006, dated September 5, 2007.

The evaluation determined that the product meets the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

In addition to the information provided in Section 6, Clarification of Scope, the Validators note the following:

In order to ensure Common Criteria EAL2 compliance, a Lexmark service representative must visit the customer site and configure the MFP in a manner consistent with the evaluated configuration. This ensures that the security settings are appropriately configured, and the appropriate TOE software version is in use.

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in the Evaluation Technical Report for the Lexmark X642e and X644e Multifunction Printer (MFP. The Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

11. Security Target

The Lexmark X642e and X644e Multifunction Printer (MFP) Security Target, Document No. SV-0606-003(1.9), dated August 31, 2007 is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
MFP	Multi-Function Peripheral
HDD	Hard Disk Drive
ISO	International Standards Organisation

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.3, dated August 2005
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.3, dated August 2005
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.3, dated August 2005

- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.3, dated August 2005
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000