National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Lexmark X463 (LR.BS.P311CCa), X464 (LR.BS.P311CCa), X651 (LR.MN.P311CCa), X652 (LR.MN.P311CCa), X654 (LR.MN.P311CCa), X734 (LR.FL.P311CCa) and X736 (LR.FL.P311CCa) Multi-Function Printers and InfoPrint 1930 MT-Model 4569-g01, g02 (LR.BS.P311CCa), 1940 MT-Model 4570-g11, g12 (LR.BS.P311CCa), 1850 MT-Model 4548-g01, g02 (LR.MN.P311CCa), 1860 MT-Model 4566-gn1, gn2 (LR.MN.P311CCa), 1870 MT-Model 4567-gn1, gn2 (LR.MN.P311CCa), Color 1846 MT-Model 4913-gd1, gd2 (LR.FL.P311CCa), and Color 1856 MT-Model 4914-gd1, gd2 (LR.FL.P311CCa) Multi-Function Printers.

Report Number: CCEVS-VR-VID10369-2011

Dated: 3 February 2011

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerry Myers
Ken Eggers

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 following Lexmark Multi-Function Printers (MFPs) at EAL3+:

- X463 (LR.BS.P311CCa),
- X464 (LR.BS.P311CCa),
- X651 (LR.MN.P311CCa),
- X652 (LR.MN.P311CCa),
- X654 (LR.MN.P311CCa),
- X734 (LR.FL.P311CCa) and
- X736 (LR.FL.P311CCa)

and the following InfoPrint Multi-Function Printers at EAL3+:

- 1930 MT-Model 4569-g01, g02 (LR.BS.P311CCa),
- 1940 MT-Model 4570-g11, g12 (LR.BS.P311CCa),
- 1850 MT-Model 4548-g01, g02 (LR.MN.P311CCa),
- 1860 MT-Model 4566-gn1, gn2 (LR.MN.P311CCa),
- 1870 MT-Model 4567-gn1, gn2 (LR.MN.P311CCa),
- Color 1846 MT-Model 4913-gd1, gd2 (LR.FL.P311CCa), and
- Color 1856 MT-Model 4914-gd1, gd2 (LR.FL.P311CCa).

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 2 February 2011. 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 3.1, Revision 2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 3+ resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is any of the Lexmark MFPs and InfoPrint MFPs with model identifiers specified above.

The MFPs 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.

The major security features of the TOE are:

- All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
- Administrators authorize Users to use the functions of the TOE.
- User Document Data are protected from unauthorized disclosure or alteration.
- User Function Data are protected from unauthorized alteration.

- TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
- TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
- Document processing and security-relevant system events are recorded, and such records are protected from disclosure or alteration by anyone except for authorized personnel.

The TOE provides the following security functionality:

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 The TOE supports I&A with a per-user selection of internal accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment). PKI authentication may also be specified, in which case all authentication must use PKI. A Backup Password mechanism may also be enabled.

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

Management Through the touch panel, 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.

User Data Buffer 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.

Self Test During initial start-up, the TOE performs self tests on its hardware components and the integrity of the building blocks and security templates.

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.

2.1 Product Identification

Identification for this evaluation is included in Table 1 Evaluation Identifier, below.

Table 1 - Evaluation Identifier

Lexmark MFP Models: • X463 (LR.BS.P311CCa), • X464 (LR.BS.P311CCa), • X651 (LR.MN.P311CCa), • X652 (LR.MN.P311CCa), • X654 (LR.MN.P311CCa), • X734 (LR.FL.P311CCa) and • X736 (LR.FL.P311CCa) and InfoPrint MFP Models: • 1930 MT-Model 4569-g01, g02 (LR.BS.P311CCa), • 1940 MT-Model 4570-g11, g12 (LR.BS.P311CCa), • 1850 MT-Model 4548-g01, g02 (LR.MN.P311CCa), • 1860 MT-Model 4566-gn1, gn2 (LR.MN.P311CCa), • 1870 MT-Model 4567-gn1, gn2 (LR.MN.P311CCa), • Color 1846 MT-Model 4913-gd1, gd2 (LR.FL.P311CCa), and • Color 1856 MT-Model 4914-gd1, gd2 (LR.FL.P311CCa).	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme

TOE	Lexmark MFP Models: - X463 (LR.BS.P311CCa), - X464 (LR.BS.P311CCa), - X651 (LR.MN.P311CCa), - X652 (LR.MN.P311CCa), - X654 (LR.MN.P311CCa), - X734 (LR.FL.P311CCa) and - X736 (LR.FL.P311CCa) and InfoPrint MFP Models: - 1930 MT-Model 4569-g01, g02 (LR.BS.P311CCa), - 1940 MT-Model 4570-g11, g12 (LR.BS.P311CCa), - 1850 MT-Model 4548-g01, g02 (LR.MN.P311CCa), - 1860 MT-Model 4566-gn1, gn2 (LR.MN.P311CCa), - 1870 MT-Model 4567-gn1, gn2 (LR.MN.P311CCa), - Color 1846 MT-Model 4913-gd1, gd2 (LR.FL.P311CCa), and - Color 1856 MT-Model 4914-gd1, gd2 (LR.FL.P311CCa) .
Protection Profile	PP Identification: 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A, version 1.0, dated January 2009 PP Conformance: - “2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A,” - “2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A,” - “2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A,” - “2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A,” - “2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A,” and - “2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A”

Security Target	Lexmark X463, X464, X651, X652, X654, X734 and X736 Multi-Function Printers And InfoPrint 1930, 1940, 1850, 1860, 1870, Color 1846, Color 1856 Multi-Function Printers Security Target, Version 2.5, Dated October 21, 2010
Evaluation Technical Report	Evaluation Technical Report for the Lexmark Multi-Function Printers and InfoPrint Multi-Function Printers with No Hard Drives, Document No. E3-0710-013(4), Dated October 27, 2010
Conformance Result	Part 2 extended and Part 3 conformant
Version of CC	CC Version 3.1 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on August 20, 2009.
Version of CEM	CEM Version 3.1 and all applicable NIAP and International Interpretations effective on August 20, 2009.
Sponsor	Lexmark International, Inc. 740 New Circle Road Lexington, KY 40550
Developer	Lexmark International, Inc. 740 New Circle Road Lexington, KY 40550
Evaluator(s)	**COACT Incorporated** Greg Beaver Pascal Patin David J. Cornwell Douglas Spoerl Brian Pleffner
Validator(s)	**NIAP CCEVS** Jerry Myers Ken Eggers

2.2 Applicable Interpretations

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

NIAP Interpretations

None

International Interpretations

None

3 TOE Description

The TOE provides the following functions related to MFPs:

- Printing – producing a hardcopy document from its electronic form
- Scanning – producing an electronic document from its hardcopy form
- Copying – duplicating a hardcopy document
- Faxing – scanning documents in hardcopy form and transmitting them in electronic form over telephone lines, and receiving documents in electronic form over telephone lines and printing them in hardcopy form

All of the MFPs included in this evaluation provide the same security functionality. Their differences are in the speed and type (color or monochrome) of printing. For the InfoPrint MFPs, a common brand name is used for MFPs both with and without a hard drive. Therefore, the MT-Model is also included in the specification to limit the MFPs in this evaluation to only those not including a hard drive. Multiple MT-Models are listed since they distinguish options such as staplers and paper tray sizes.

4 Assumptions

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

Table 2 - Assumptions

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.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.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.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.

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.

Table 3 - Threats

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

6 Organizational Security Policies

This section describes the Organizational Security Policies (OSPs) that apply to the TOE.

Table 4 - Organizational Security Policies

Name	Definition
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 input-output interfaces of the TOE, operation of the interfaces will be controlled by the TOE and its operational environment.
P.SOFTWARE.VERIFICATION	To detect unintentional malfunction of the TSF, procedures will exist to self-verify TSF data
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner

7 High Level Description of Product Security Functionality

The TOE provides the following security functionality:

7.1 Audit Generation

The TOE generates audit event records for security-relevant events. A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated. The time field is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured. As audit event records are generated, they are forwarded to the remote syslog IT system configured by an administrator.

7.2 Identification and Authentication

Users are required to successfully complete the I&A process before they are permitted to access any restricted functionality. The set of restricted functionality is under the control of the administrators, with the exception of submission of network print jobs which is also allowed. The I&A process is controlled by security templates that are associated with functions and menus. Each security template specifies two building blocks – one for authentication and the second for authorization. The security template also includes a list of groups that are authorized to perform the function or access the menu that the security template is associated with. When I&A is necessary, the TOE examines the authentication building block in the security template to determine what authentication mechanism should be used. The general purpose mechanisms supported in the evaluated configuration are PKI authentication, Internal Accounts and LDAP+GSSAPI.

In the case of failed validations, an error message is displayed on the touch panel, and then the display returns to the previous screen for further user action. An audit record for the failed authentication attempt is generated.

If validation is successful, the TOE binds the username, password, account name, email address, group memberships (for Internal Accounts only) and name of the building block used for authentication to the user session for future use (only the username and group memberships are security attributes). An audit record for the successful authentication is generated.

The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for actions on the Home screen of the touch panel expires. If the inactivity timer expires, an audit record is generated.

If a user locks the touch panel, the user session is terminated immediately. Similarly, after a user unlocks the touch panel, the user session is terminated immediately.

7.3 Access Control

Access control validates the user access request against the authorizations configured by administrators for specific functions. On a per-item basis, authorization may be configured as “disabled” (no access), “no security” (open to all users), or restricted (via security templates) (some items do not support all three options).

Authorization is restricted by associating a security template with an item. The security template assigned to each item may be the same or different as the security template(s) assigned to other items. Each security template points to an authentication building block as well as an authorization building block; the two building blocks may be the same or different.

The following summarizes the access controls and configuration parameters used by the TOE to control user access to the MFP functions provided by the TOE

- Printing – Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded. Submitted jobs are always held on the TOE until released or deleted by a user authorized for the appropriate access control and whose userid matches the username specified when the job was submitted. Scanning (to Fax or Email)

- Scanning - may be performed as part of a fax or email function. Only authorized users may perform scans. Scanning for fax is allowed if the Enable Fax Scans configuration parameter is "On" and the user is authorized for the Fax Function access control. Scanning for email is allowed if the user is authorized for the E-mail Function access control.

- Copying - allowed if the user is authorized for the Copy Function access control. A user may view or delete their own copy jobs queued for printing.

- Incoming faxes - allowed if the "Enable Fax Receive" (for analog fax mode) or "Enable Fax Receive" (for fax server mode) configuration parameter is "On". Incoming faxes are always held in the queue (until released) in the evaluated configuration. Only users authorized for the Release Held Faxes access control may release or delete the faxes.

7.4 Management

The TOE provides the ability for authorized administrators to manage TSF data. Authorization is granular, enabling different administrators to be granted access to different TSF data. When an administrator modifies TSF data, an audit record is generated.

The following touch panel menus are organized by the administrator menu structure: Reports Menu, Network/Ports Menu, Security Menu, Settings Menu, Fax Settings Menu, Email Settings Menu, Print Settings/Setup Settings Menu,

The security reset jumper provides an alternate mechanism to manage some TSF data. The TOE contains a hardware jumper that can be used to:

- erase all security templates, building blocks, and access controls that a user has defined (i.e. the factory default configuration); OR
- force the value of each function access control to "No Security" (all security templates and building blocks are preserved but not applied to any function).

7.5 Fax Separation

The Fax Separation 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 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 (in the evaluated configuration) is a document that was scanned for faxing.

7.6 User Data Buffer Wiping

The TOE overwrites RAM with a fixed pattern upon deallocation of any buffer used to hold user document data.

7.7 Secure Communications

IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are TDES, AES and DES. Both SHA-1 and MD5 are supported for HMACs. ISAKMP and IKE are used to establish the Security Association (SA) and session keys for the IPSec exchanges. Diffie-Hellman is used for key agreement, using Oakley Groups 1, 2 or 14. During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature for it is validated.

If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded.

7.8 Self Test

During initial start-up, the TOE performs self tests on the hardware. The integrity of the security templates and building blocks is verified by ensuring that all the security templates specified in access controls exist and that all building blocks referenced by security templates exist.

If any problems are detected with the hardware, an appropriate error message is posted on the touch screen and operation is suspended. If a problem is detected with the integrity of the security templates or building blocks, the data is reset to the factory default, an audit log record is generated, an appropriate error message is posted on the touch screen, and further operation is suspended. In this case, a system restart will result in the system being operational with the factory default settings for the data.

8 Clarification of Scope

The Target of Evaluation (TOE) is described using the standard Common Criteria terminology of Users, Objects, Operations, and Interfaces. Two additional terms are introduced:

- Channel describes both data interfaces and hardcopy document input/output mechanisms, and
- TOE Owner is a person or organizational entity responsible for protecting TOE assets and establishing related security policies.

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrator.

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. Objects are equivalent to TOE Assets. There are three categories of Objects: User Data, TSF Data, and Functions.

- User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two types of objects: User Document Data, and User Function Data.

- TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two types of objects: TSF Protected Data and TSF Confidential Data.

- Functions perform processing, storage, and transmission of data that may be present in the TOE. These functions are described below

    - Printing: a function in which electronic document input is converted to physical document output

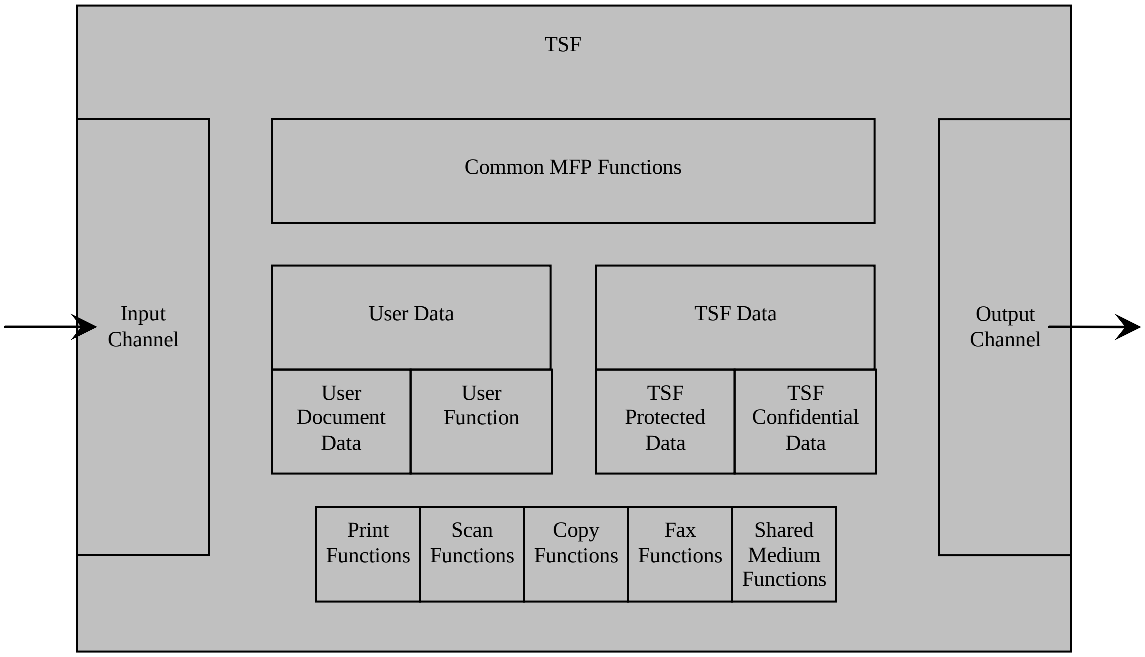
    - Scanning: a function in which physical document input is converted to electronic document output

    - Copying: a function in which physical document input is duplicated to physical document output

    - Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output

    - Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which is or can be shared by other users, such as wired or wireless network media and most radio-frequency wireless media

Figure 1 - TOE Model



9 Architecture Information

The following configuration options apply to the evaluated configuration of the TOE:

- The TOE includes the single Ethernet interface that is part of the standard configuration of every MFP model. No optional network interfaces are installed.
- No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.
- All USB ports on the MFPs that perform document processing functions are disabled. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If PKI authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. If a card reader is installed, the PKI authentication functionality is the only I&A mechanism that can be used.
- All management functions are performed via the touch screen panel and the HTTP(S) server (for remote management) is disabled. This is done to align the TOE with the P2600 protection profiles currently in development, which require many operations to be performed locally (via the touch screen panel). In addition, this mechanism is preferred over remote management capability because it requires physical access to the TOE, is more resistant to brute force password attacks, and precludes network-based attacks on the management functions.
- Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.
- All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged. Certificates presented by remote IT systems are validated.
- Support for AppleTalk, NetWare (IPX) and LexLink are disabled since these protocols do not provide confidentiality and integrity protection.
- I&A may use Internal Accounts and/or LDAP+GSSAPI on a per-user basis. The Backup Password mechanism may be enabled at the discretion of the administrators. If PKI authentication is used, all I&A must use the PKI authentication mechanism. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.
- LDAP+GSSAPI and PKI authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific MFP. Binds to LDAP servers for PKI authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.

- Internal Accounts require both User ID and password (rather than just User ID).
- Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.
- User data sent by the MFP in email messages is sent as an attachment (not as a web link).
- No Java applications are loaded into the MFP by Administrators. These applications are referred to as LES applications in end user documentation. The following LES applications are installed by Lexmark before the TOE is shipped: “PKI Authentication”, “PKI Held Jobs”, and “CAC Smartcard Authentication Token”.
- No option card for downloadable emulators is installed in the TOE.
- Incoming faxes are always held until released by an authorized administrator.
- Some form of credentials (device or user) is required to authenticate to the SMTP server.
- Fax forwarding is disabled to limit the destinations for incoming faxes to the local printer only.
- NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
- All administrators must be authorized for all of the document processing functions (print, copy, scan, fax).
- All network print jobs are held until released. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.
- Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Internal Accounts and the Backup Password:
  - A minimum of 8 characters
  - At least one lower case letter, one upper case letter, and one non-alphabetic character
  - No dictionary words or permutations of the user name
- All unnecessary network ports are disabled.

The following identifies the minimum hardware and software requirements for components provided by the IT Environment:

The TOE is a complete MFP, including the firmware and hardware. To be fully operational, any combination of the following items may be connected to the TOE:

- 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 PKI 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:

    - Omnikey 5121 SmartCard Reader,

    - Omnikey 5321 SmartCard Reader,

    - Omnikey 5125 SmartCard Reader,

    - 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), and

    - SCM SCR 331.

10 Product Delivery

10.1 Delivery of Hardware Components

Fulfillment centers receive hardware shipments from the factory in sealed containers. The centers are responsible for integration of the hardware, installation of the firmware, and shipment to the customer.

The centers have secure real-time communication with the Lexmark corporate facilities to ensure they have the latest customer orders and Engineering Change Orders (ECOs). The real-time communication is also used to send order status updates back to the corporate servers (status updates for InfoPrint customers are relayed via Lexmark corporate servers). If connectivity is lost, the centers are allowed to operate autonomously for up to 18 hours. If connectivity is not restored within that time, processing at that center must be suspended.

Firmware images are supplied to the fulfillment centers after they have been approved for release. The proprietary Manufacturing Execution System (MES) tool is responsible for coordinating the distribution of the images to the fulfillment centers.

The part number specified in the customer order directs the fulfillment center to install the evaluated version of firmware on the MFPs when specified by the customer. Orders are received directly by Lexmark for Lexmark customers. For InfoPrint customers, the order is first received by InfoPrint and then electronically forwarded to Lexmark over a VPN. Different part numbers are used to distinguish between equivalent Lexmark and InfoPrint models. The proprietary Orion tool is used within the fulfillment centers to ensure the appropriate firmware is installed during the fulfillment process.

Each shipment includes a documentation CD as well as a hard-copy version of the Common Criteria Installation supplement and administrator guide. Masters for these items are supplied to the fulfillment centers after they have been approved for release. They are reproduced as needed by the fulfillment center to satisfy orders. The part number on the order specifies whether Lexmark-branded or InfoPrint-branded materials are included in the shipment.

Reputable carriers that provide internet tracking capabilities are used for shipments to the customers.

The following documentation is delivered with the TOE:

No Hard Drive MFP -- X463

- Setup Guide – 30484760001 (Hard Copy)
- Common Criteria Installation Supplement and Administrator Guide (Hard Copy)
- Lexmark X46x Series User's Guide (Soft Copy)
- Quick Reference Guide (Soft Copy)
- Lexmark Networking Guide (Soft Copy)

Of the delivered documents identified above, the following documents were reviewed as part of this evaluation:

- Lexmark X46x Series User's Guide (Soft Copy) This user guide is specific to the MFP delivered. The delivery of each MFP includes the delivery of the specific user manual associated with that MPF product.
- Common Criteria Installation Supplement and Administrator Guide (Hard Copy)CCTL

10.2 Verifying Integrity of Hardware and Firmware Components

The reputable carriers used for shipments ensure continuous control of the packages during shipment. The shipping documentation received with an MFP identifies Lexmark or InfoPrint (as appropriate) as the source of the shipment. Customers may verify this information via the shipper’s web site.

The version number of software installed on the MFP may be printed once it is operational to ensure the evaluated version is installed.

The Common Criteria Installation supplement and administrator guide provides the following instructions to verify the physical interfaces and installed firmware.

- Inspect the MFP to verify that only one network interface is installed. There should be no optional network, parallel, or serial interfaces. Note: USB ports that perform document processing functions are disabled at the factory.

- Turn the MFP on using the power switch.

- From the home screen touch Menus > Reports > Menu Settings Page. Several pages of device information will print.

- Under Installed Features, verify that no Download Emulator (DLE) option cards have been installed.

- If you find additional interfaces, or if a DLE card has been installed, contact your Lexmark representative before proceeding.

- To verify the firmware version, under Device Information, locate Base =, and Network =.

- Contact your Lexmark representative to verify that the Base and Network values are correct and up-to-date.

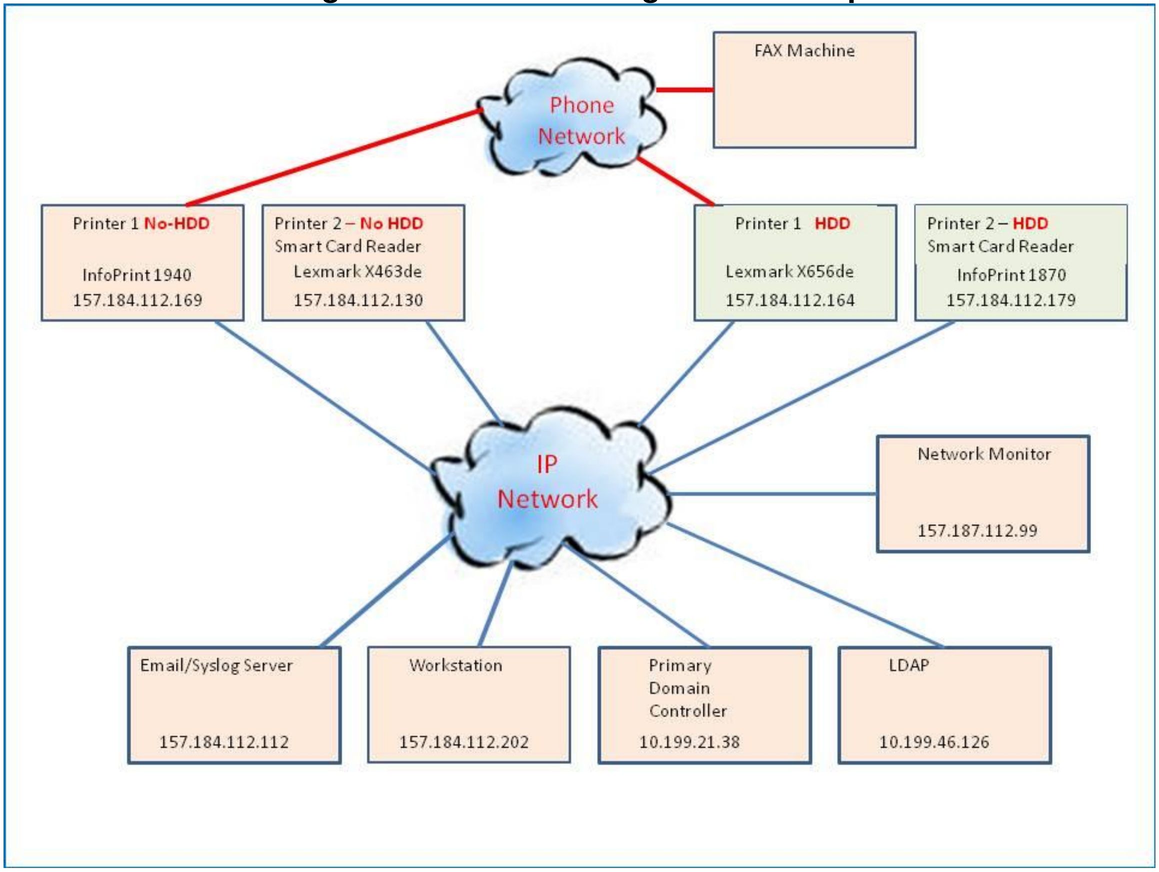
11 IT Product Testing

Testing was completed on October 27, 2010 at the COACT CCTL in Columbia, Maryland and at Lexmark International, Inc. in Lexington, KY. COACT employees performed the tests.

11.1 Evaluator Functional Test Environment

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

Figure 2 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 5 - Test Configuration Overview

System	Purpose
Workstation	This system is configured to send print jobs to Printer 1 and to exchange email with the Email Server.
Primary Domain Controller	This system acts as the Primary Domain Controller for the network, providing Active Directory, Kerberos, GSSAPI, DNS, NTP, and PKI services.
Email/Syslog Server	This system provides an SMTP server capable of receiving email from Printer 1 and forwarding it to a user on Workstation, and a Syslog server capable of receiving and displaying Syslog messages from Printer 1 and Printer 2. This system may be combined with Primary Domain Controller.

System	Purpose
IP Network	An IP network (either IPv4 or Ipv6) that is able to send a copy of the traffic between Workstation and Printer 1 to Network Monitor.
Printer 1	One instance of the TOE (either a Lexmark or InfoPrint model) without a Smart Card reader.
Printer 2	Second instance of the TOE (either a Lexmark or InfoPrint model) with a Smart Card reader.
Phone Network	Analog telephone network providing connectivity between Printer 1 and Fax Machine. This may be the Public Switched Telephone Network (PSTN) or Private Branch Exchange (PABX) or Telephone Line Emulator (TLE).
Fax Machine	Fax machine capable of exchanging faxes with Printer 1 via the Phone Network.
Network Monitor	This system is used to act as the attack PC for the penetration tests and network monitoring.

The following tables provide more information about the systems and configuration information specific to the test procedures. The configuration information consists of user accounts, user groups, and security templates to be used for the tests. All active systems connected to IP Network are configured to use IPSec.

Table 6 - Workstation Requirements

Description	Test Configuration Specific Details
Authorized Users Permitted	“user1”

Table 7 - Primary Domain Controller

Description	Test Configuration Specific Details
AD Users/Groups	User “test” that is a member of group “Test_Group” User “test1” that is not a member of group “Test_Group” CAC user “cac1” that is a member of group “CAC_Group” CAC user “cac2” that is not a member of group “CAC_Group” CAC user “admin” that is a member of group “Administrators”
DNS Configuration	Entries for all active systems connected to IP Network
NTP Configuration	Acting as server No authentication required

Table 8 - Email/Syslog Server

Description	Test Configuration Specific Details
Syslog Configuration	Receive via UDP
Email Configuration	No credentials required to send Email

Table 9 - Printer 1 Requirements

Description	Test Configuration Specific Details
Internal Account Groups	“Administrators” “Users”

Description	Test Configuration Specific Details
	“Restricted”
Internal Account Users	User “admin” as a member of “Administrators” User “user1” as a member of “Users” User “user2” as a member of “Users” User “user3” as a member of ”Restricted”
LDAP+GSSAPI Configuration	LDAP+GSSAPI building block named “LDAPGSSAPI” with server Primary Domain Controller
Kerberos Configuration	KDC Address: Primary Domain Controller KDC Port: Kerberos port on Primary Domain Controller Realm: Realm configured on Primary Domain Controller
Security Templates	“Administrators_Only” with “Internal_Accounts_Building_Block” for authentication and authorization and group “Administrators” “Authorized_Users” with “Internal_Accounts_Building_Block” for authentication and authorization and group “Users” “LDAPGSSAPI_Users” with “LDAPGSSAPI” for authentication and authorization and group “Test_Group”
User Functions Enabled	Fax, Email
Function Access Controls	E-mail: LDAPGSSAPI_Users Fax: Authorized_Users Solution 1: Authorized_Users All FACs restricted to Administrators: Administrators_Only
Fax Configuration	Enable Fax Receive: On Fax Mode: Analog
Email Configuration	Primary SMTP Gateway: Email/Syslog Server Primary SMTP Gateway Port: Port used on Primary Domain Controller SMTP Server Authentication: No authentication required User-Initiated E-mail: None
Security Audit Logging Configuration	Remote Syslog Server: Email/Syslog Server Remote Syslog Method: Normal UDP
NTP Configuration	Enable NTP: On NTP Server: Primary Domain Controller

Table 10 - Printer 2 Requirements

Description	Test Configuration Specific Details
CAC Configuration	Use MFP Kerberos Setup: Set DC Validation Mode: Device Certificate Validation A Certificate Authority certificate must be installed
Kerberos Configuration	KDC Address: Primary Domain Controller KDC Port: Kerberos port on Primary Domain Controller Realm: Realm configured on Primary Domain Controller
Security Templates	“Administrators_Only” with “PKI_Auth” for authentication and authorization and group “Administrators” “CAC_Users” with “PKI_Auth” for authentication and authorization and group “CAC_Group”
User Functions Enabled	Copy
Function Access Controls	Copy: CAC_Users All other required FACs: Administrators_Only
Security Audit Logging Configuration	Remote Syslog Server: Email/Syslog Server Remote Syslog Method: Normal UDP
NTP Configuration	Enable NTP: On NTP Server: Primary Domain Controller

Table 11 - Network Monitor

Description	Test Configuration Specific Details
Penetration and Attack Tools	Windows XP Professional SP3 Internet Explorer 8.0.6001.18702 Firefox 3.6.8 WinZip 10 ZENMAP GUI 5.21 SnagIt 8 WireShark 1.4.0 Nessus Version 4.2 Revision 11 Paros Proxy 3.2.13

11.2 Functional Test Results

The repeated developer test suite includes all of the developer functional tests. Additionally, each of the Security Function and developer tested TSFI are included in the CCTL test suite. Results are found in the Lexmark Multi-Function Printers and InfoPrint Multi-Function Printers without Hard Drives Test Report, Document No. E3-0610-011(4), Dated October 27, 2010.

11.3 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. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

11.4 Evaluator Penetration Tests

The evaluator examined sources of information publicly available to support the identification of possible potential vulnerabilities in the TOE.

The sources of the publicly available information are provided below.

- http://cve.mitre.org – Entries found for older versions
- http://google.com
- http://osvdb.org/ -
- http://www.securityfocus.com/ - Same vulnerabilities as on CVE
- http://secunia.com/ - Same vulnerabilities as on CVE
- http://www.us-cert.gov – Nothing found
- http://securitytracker.com/ - Same vulnerabilities as on CVE
- http://web.nvd.nist.gov – Same vulnerabilities as on CVE

- http://www.securityspace.com/ - Same vulnerabilities as on CVE
- http://www.cvedetails.com/
- https://www.juniper.net/security/auto/vulnerabilities/vuln6047.html
- https://www.infoprintsolutionscompany.com/internet/comnelit.nsf/Files/pjl_advisory_032210/$File/pjl_advisory_032210.pdf
- https://www.infoprintsolutionscompany.com/internet/comnelit.nsf/Files/ftp_advisory_032210/$File/ftp_advisory_032210.pdf

As noted in the list above, many of the vulnerabilities found through publicly available information referred back to the CVE entries. All of the vulnerabilities were mitigated or not directly related to the TOE and its intended environment. No other vulnerabilities were found.

The evaluator performed the public domain vulnerability searches using the following key words.

- Lexmark
- X463
- X464
- X651
- X652
- X654
- X734
- X736
- Infoprint
- 1930
- 1940
- 1850
- 1860
- 1870
- 1846
- 1856
- Linux 2.6.18

These keywords were chosen since they include the developer name and model numbers of the TOE. The TOE MFP incorporates a heavily customized version of the Linux 2.6.18 kernel for the O/S. Therefore, this version of Linux was also checked for publicly available sources of vulnerability information.

The evaluator used additional keywords listed below to search for vulnerabilities:

- Multi-function

- Printer
- LaserJet
- HP
- M3530
- CP3525

The keywords not related to the TOE were chosen since the TOE is a similar product (i.e. Multi Function Printer).

11.5 Test Results

The end result of the functional testing activities was that all tests gave expected (correct) results.

The evaluator penetration tests revealed the following:

- A Denial of Service was observed if a specific pattern of events was followed in the usage of the MFP Shortcuts.

- Though not claiming FIPS 140-2 compliance, a software code review revealed that the TOE did not zeroize the encryption keys and that the random number generator did not use the ANSI X9.31 RNG.'

The MFP firmware was modified as a result of the Common Criteria testing. The code was changed from version P311CC to P311CCa.

The changes addressed the following:

- A Penetration Test revealed a Denial of Service vulnerability.

  No vulnerabilities were identified by the use of shortcuts by the users, since each user had to authenticate to access each function. However, a Denial of Service was observed if a specific pattern of events was followed in the usage of the MFP Shortcuts. It was noted that after a shortcut was selected and no user authentication was entered, the MFP would time out and return to the Home screen as expected. However, the Home screen was frozen and selecting any of the icons (i.e. Copy, Fax, Email) had no effect. Only selecting the "Release Print Jobs" button would unlock the MFP Home screen and normal operation could be resumed. The firmware update addressed and corrected the issue.

- Evaluator Test Analysis of the Key Zeroization Methodology revealed that the encryption keys were not zeroized.

  The following summarizes the key zeroization after the firmware updates.

  - The RSA private key is not zeroized.

  - The 256 bit Disk Encryption Key is zeroized when disk encryption is turned off.

  - The IPSEC session keys and Diffie-Hellman keys are zeroized.

- Evaluator TestAnalysis of the ANSI X9.31 Appendix A.2.4 RNG, revealed that the random number generator did not use ANSI X9.31.
  The following summarizes the random number generation after the firmware updates.

  The version of OpenSSL code used by the TOE is 0.9.8.d. This code has been supplemented with the ANSI X9.31 RNG from the OpenSSL version 1.2. The main functions and subfunctions of the ANSI X9.31 RNG have been implemented. It was verified from source code that the ANSI X9.31 RNG is used to generate keys for the following algorithms:

  - DES
  - TDES
  - AES
  - HMAC

The testing of the updated firmware revealed 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.

12 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 product for selected 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 Multi-Function Printers and InfoPrint Multi-Function Printers without Hard Drives Test Report, Document No. E3-0610-011(4), Dated October 27, 2010

The evaluation determined that the product meets the requirements for EAL 3+. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. Validator Comments

None.

11. Security Target

Lexmark X463, X464, X651, X652, X654, X734 and X736 Multi-Function Printers And InfoPrint 1930, 1940, 1850, 1860, 1870, Color 1846, Color 1856 Multi-Function Printers Security Target, Version 2.5, Dated October 21, 2010

12. List of Acronyms

AES	Advanced Encryption Standard
AIO	All In One
BSD	Berkeley Software Distribution
CAC	Common Access Card
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GSSAPI	Generic Security Services Application Program Interface
HTTP	HyperText Transfer Protocol
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
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	MegaByte
MFD	Multi-Function Device
MFP	Multi-Function Printer
NTP	Network Time Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PJL	Printer Job Language
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request For Comments
SASL	Simple Authentication and Security Layer
SFP	Security Function Policy
SFR	Security Functional Requirement

SMTP	Simple Mail Transport Protocol
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus

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 3.1, Revision 2, dated September 2007
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 3.1, Revision 2, dated September 2007
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 3.1, Revision 2, dated September 2007
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 3.1, Revision 2, dated September 2007
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000