National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Lexmark MX511h(LW20.SB4.P231CC), MX611h(LW20.SB7.P231CC), MX710h(LW20.TU.P231CC), MX711h(LW20.TU.P231CC), MX810(LW20.TU.P231CC), MX811(LW20.TU.P231CC), MX812(LW20.TU.P231CC), XM7155(LW20.TU.P231CC), XM7163(LW20.TU.P231CC), XM7170(LW20.TU.P231CC), CX510h(LW20.GM7.P231CC) and XC2132(LW20.GM7.P231CC) Multi-Function Printers

Report Number: CCEVS-VR-VID10510-2014
Dated: 31 January 2014
Version: 1.0

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

Mike Allen (Lead Validator)
Jerome F. Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

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 is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Lexmark MX511h(LW20.SB4.P231CC), MX611h(LW20.SB7.P231CC), MX710h(LW20.TU.P231CC), MX711h(LW20.TU.P231CC), MX810(LW20.TU.P231CC), MX811(LW20.TU.P231CC), MX812(LW20.TU.P231CC), XM7155(LW20.TU.P231CC), XM7163(LW20.TU.P231CC), XM7170(LW20.TU.P231CC), CX510h(LW20.GM7.P231CC) and XC2132(LW20.GM7.P231CC) Multi-Function Printers with Hard Drives. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Lexmark Printers was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed in January 2014.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the associated test report. The ST was written by Common Criteria Consulting LLC for Lexmark. The ETR and test report used in developing this validation report were written by COACT. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, dated September 2012 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R4, dated September 2012. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Lexmark Multi-Function Printers with Hard Drives Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is Lexmark MX511h(LW20.SB4.P231CC), MX611h(LW20.SB7.P231CC), MX710h(LW20.TU.P231CC), MX711h(LW20.TU.P231CC), MX810(LW20.TU.P231CC), MX811(LW20.TU.P231CC), MX812(LW20.TU.P231CC), XM7155(LW20.TU.P231CC), XM7163(LW20.TU.P231CC), XM7170(LW20.TU.P231CC), CX510h(LW20.GM7.P231CC) and XC2132(LW20.GM7.P231CC) Multi-Function Printers with Hard Drives.

The TOE provides the following functions related to MFPs.

1. Printing – producing a hardcopy document from its electronic form.
2. Scanning – producing an electronic document from its hardcopy form.
3. Copying – duplicating a hardcopy document.
4. Faxing – scanning documents in hardcopy form and transmitting them in electronic form over telephone lines, and receiving documents in electronic form over telephone line and printing them in hardcopy form.

All of the models included in the evaluation are complete MFPs in a single self-contained unit. All of the MFPs included in this evaluation provide the same security functionality. Their differences are in the speed of printing and support for colour operations.

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. Remote management can be accomplished through the MFPs Embedded Web Server.

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
2. Administrators authorize Users to use the functions of the TOE.
3. User Document Data are protected from unauthorized disclosure or alteration.
4. User Function Data are protected from unauthorized alteration.
5. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
6. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
7. 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 COACT evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2) have been met.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

1.1 Applicable Interpretations

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

NIAP Interpretations

None

International Interpretations

None

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, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring 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's Product Compliant 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 Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Lexmark MX511h(LW20.SB4.P231CC), MX611h(LW20.SB7.P231CC), MX710h(LW20.TU.P231CC), MX711h(LW20.TU.P231CC), MX810(LW20.TU.P231CC), MX811(LW20.TU.P231CC), MX812(LW20.TU.P231CC), XM7155(LW20.TU.P231CC), XM7163(LW20.TU.P231CC), XM7170(LW20.TU.P231CC), CX510h(LW20.GM7.P231CC) and XC2132(LW20.GM7.P231CC) Multi-Function Printers with Hard Drives
Protection Profiles	U.S. Government Protection Profile for Hardcopy Devices (IEEE Std. 2600.2™-2009), dated February 26, 2010, version 1.0, including the augmentations specified by Attachment A of CCEVS Policy Letter #20 dated 15 November 2010. "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B," "2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B," "2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B," "2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B," "2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B," and "2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B".
Security Target	*Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Security Target*, Version 1.10, January 8, 2014

Dates of evaluation	October 2012 through January 2014
Evaluation Technical Report	*Lexmark Hard Drive Printers Evaluation Technical Report*, January 10, 2014, Document No. E2-0513-008
Conformance Result	Part 2 extended and Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R4, September 2012 and all applicable NIAP and International Interpretations effective on October 10, 2012.
Common Evaluation Methodology (CEM) version	CEM version 3.1R4 dated September 2012 and all applicable NIAP and International Interpretations effective on October 10, 2012.
Sponsor	Lexmark International, Inc., 740 New Circle Road, Lexington, KY 40550
Developer	Lexmark International, Inc., 740 New Circle Road, Lexington, KY 40550
Common Criteria Testing Lab	COACT Inc., Columbia, MD
Evaluators	Rachel Lisi and Rory Saunders
Validation Team	Jerome F. Myers and Mike Allen of the Aerospace Corporation

3 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Identification and authentication
3. Access Control
4. Management
5. Operator Panel Lockout
6. FAX Separation
7. Hard Disk Encryption
8. Disk Wiping
9. Secure Communications
10. Self Test

3.1 Security Audit

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 a Network Time Protocol (NTP) server if external time is configured. As audit event records are generated, they are forwarded to a remote syslog IT system configured by an administrator.

3.2 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 is associated with the security template. 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 authentications, 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 authentication 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.

3.3 Access Control

Access control validates the user access request against security attributes (User/Group ID) 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:

A) 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.

B) Scanning (to Fax or Email) - 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.

C) Copying – is 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.

D) 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.

3.4 Management

The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. 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 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. return to 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).

3.5 Operator Panel Lockout

The Operator Panel Lockout function enables the touch panel to be "locked" to prevent anyone from using it until it is "unlocked" by an authorized user. This function is enabled when a security template is associated with the Operator Panel Lock access control described above. When enabled, an icon is displayed on the Home page to lock the panel.

3.6 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.

3.7 Hard Disk Encryption

All user data saved on the Hard Disk is encrypted using 256-bit AES. The types of data saved on the Hard Disk (and therefore encrypted) include buffered job data, held jobs, images referenced by other jobs, and macros. The contents of each file are automatically encrypted as they are written to the Hard Disk and automatically decrypted when the contents are read. This security function is intended to protect against data disclosure if a malicious agent is able to gain physical possession of the Hard Disk. This security function operates transparently to users and is always enabled in the evaluated configuration.

3.8 Disk Wiping

In the evaluated configuration, the TOE is configured to perform automatic disk wiping with a multi-pass method. Files containing user data are stored on the internal hard drive until they are no longer needed. At that time, they are logically deleted and marked as needing to be wiped. Until the wiping occurs, disk blocks containing the files are not available for use by any user. Every 5 seconds, the TOE checks to see if any "deleted" files are present and begins the disk wiping process.

The TOE overwrites each block associated with each deleted file (including bad and remapped sectors) three times: first with "0x0F" (i.e. 0000 1111), then with "0xF0" (i.e. 1111 0000), and

finally with a block of random data (supplied by the internal random number generator). Each time that the device wipes a different file, it selects a different block of random data. This method is compliant with NIST SP800-88 and the DSS "Clearing and Sanitization Matrix" (C&SM).

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

3.9 Secure Communications

IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provides 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, 5 or 14. During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature before it is validated.

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

3.10 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.

4 Assumptions, Threats, Policies and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the Lexmark Multi-Function Printers with Hard Drives.

4.1 Assumptions

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

Table 2: Assumptions

Assumption	Definition
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.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

4.2 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

Threat	Definition
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

4.3 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

4.4 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in the ST, with a certain level of assurance (EAL 2 augmented with ALC_FLR.2 in this case).
- This evaluation only covers the specific versions of printers identified in this document, and not any earlier or later versions released or in process or other printers from the same vendor.
- As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The following configuration options apply to the evaluated configuration of the TOE. In order to operate the TOE in the evaluated configuration, these restrictions must be followed.

1. The TOE includes the single Ethernet interface that is part of the standard configuration of every MFP model. No optional network interfaces are installed.
2. No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.
3. 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 Smart Card 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. A reader is shipped with the MFP. If Smart card authentication is not used, the card reader may be left unconnected.
4. Operational management functions are performed via browser sessions to the embedded web server or via the management menus available through the touch panel.
5. Disk encryption is enabled.
6. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.
7. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.CONF and D.PROT. Certificates presented by remote IT systems are validated.
8. Because all network traffic is required to use IPSec with ESP, syslog records sent to a remote IT system also are protected by IPSec with ESP. This is beyond IEEE Std. 2600.2™-2009 requirements for transmission of audit records.
9. Support for AppleTalk is disabled since it does not provide confidentiality and integrity protection.
10. 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. Smart Card authentication may be used for touch panel users. No other I&A mechanisms are included in the evaluated configuration because they provide significantly lower strength than the supported mechanisms.
11. LDAP+GSSAPI and Smart Card 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 Smart Card authentication use credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.
12. Internal Accounts require User ID and password (rather than just User ID).
13. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.

14. Disk wiping functionality is configured for automatic mode with a multi-pass method. This approach is the more secure form of disk wiping and is compliant with NIST SP800-88 and the DSS "Clearing and Sanitization Matrix" (C&SM).
15. User data sent by the MFP in email messages is sent as an attachment (not as a web link).
16. No Java applications are loaded into the MFP by Administrators. These applications are referred to as eSF applications in end user documentation. The following eSF applications are installed by Lexmark before the TOE is shipped and must be enabled: “eSF Security Manager”, “Smart Card Authentication”, and “Secure Held Print Jobs”.
17. The following eSF applications are installed by Lexmark before the TOE is shipped and must be enabled if smart card authentication is used: “Smart Card Authentication Client”, “PIV Smart Card Driver (if PIV cards are used)”, “CAC Smart Card Driver (if CAC cards are used)”, and “Background and Idle Screen”.
18. All other eSF applications installed by Lexmark before the TOE is shipped must be disabled.
19. No option card for downloadable emulators is installed in the TOE.
20. All fax jobs are stored on disk (rather than NAND) to ensure their contents are wiped upon completion of each job. Incoming faxes are always held until released by an authorized administrator.
21. Some form of credential (device or user) is required to authenticate to the SMTP server.
22. Fax forwarding is disabled to limit the destinations for incoming faxes to the local printer only.
23. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
24. All administrators must be authorized for all of the document processing functions (print, copy, scan, fax).
25. All network print jobs are held until released via the touch panel. 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.
26. All incoming fax jobs are held until released via the touch panel. Held print jobs may only be released by an authenticated user with the U.ADMINISTRATOR role.
27. 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
28. Simple Network Management Protocol (SNMP) support is disabled.

29. Internet Printing Protocol (IPP) support is disabled.
30. All unnecessary network ports are disabled.

5 Architectural Information

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:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.
2. A telephone line for fax capability.
3. IT systems that submit print jobs to the MFP via the network using standard print protocols.
4. IT systems that send and/or receive faxes via the telephone line.
5. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
6. LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
7. Card reader and cards to support Smart Card 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:
    a. Omnikey 3121 SmartCard Reader,
    b. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),
    c. SCM SCR 331,
    d. SCM SCR 3310v2.

The TOE provides the following functions related to MFPs:

1. Printing – producing a hardcopy document from its electronic form
2. Scanning – producing an electronic document from its hardcopy form
3. Copying – duplicating a hardcopy document
4. 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 TOE models included in the evaluation are complete MFPs in a single unit.
All of the MFPs included in this evaluation provide the same security functionality. Their differences are in the speed of printing and support for color operations. The following table summarize the technical characteristics of the models.

Table 5: Technical Characteristics of the MFP Models

Model	Processor	Color/Mono	Pages Per Minute
MX511h	ARM v7 800 MHz	Mono	45
MX611h	ARM v7 800 MHz	Mono	50
MX710h	ARM v7 800 MHz	Mono	63
MX711h	ARM v7 800 MHz	Mono	70
MX810	ARM v7 800 MHz	Mono	55
MX811	ARM v7 800 MHz	Mono	63
MX812	ARM v7 800 MHz	Mono	70
XM7155	ARM v7 800 MHz	Mono	55
XM7163	ARM v7 800 MHz	Mono	63
XM7170	ARM v7 800 MHz	Mono	70
CX510h	ARM v7 800 MHz	Color	32
XC2132	ARM v7 800 MHz	Color	32

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. In this document, the terms User and Subject are used interchangeably.

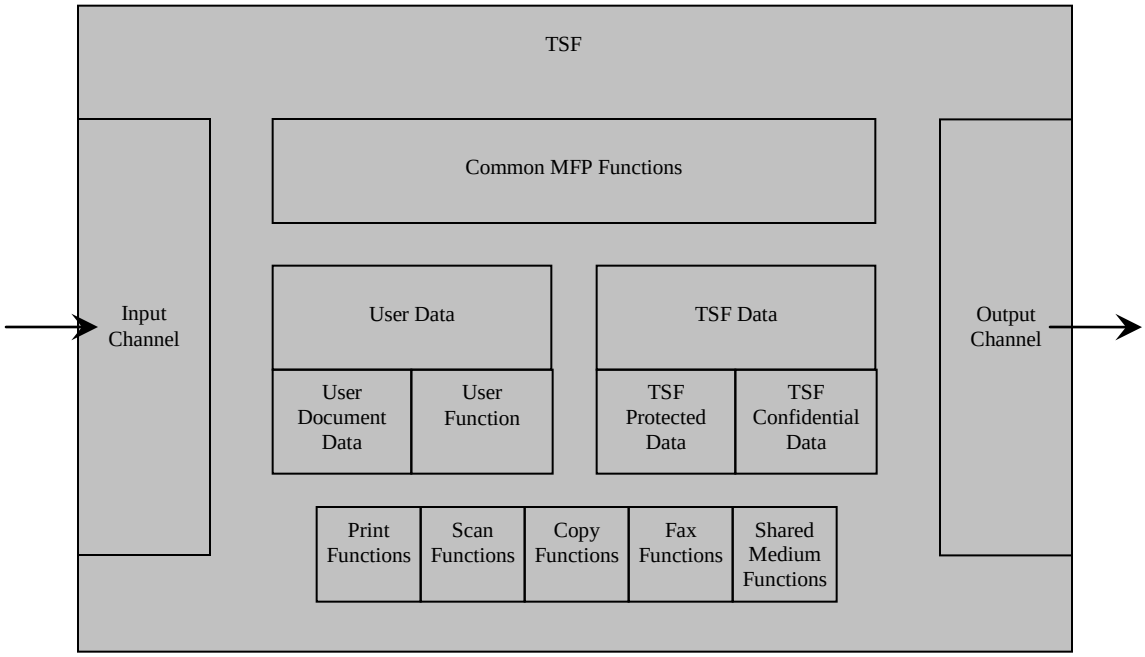

Figure 1: TOE Model

6 Documentation

The following documentation was supplied by Lexmark. All of the documentation is applicable and was used as evidence for the evaluation of the Lexmark Multi-Function Printers.

6.1 Design Documentation

- Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Security Target, Version 1.10, January 8, 2014
- Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h, and XC2132 Multi-Function Printers Security Architecture, Version 1.1, January 28, 2013
- Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Functional Specification, Version 1.3, May 6, 2013
- Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h, and XC2132 and Dell B5465 Multi-Function Printers TOE Design Specification, Version 1.1, January 28, 2013

6.2 Guidance Documentation

- Lexmark CX510 Series User's Guide, July 2012
- Lexmark Embedded Web Server — Security Administrator's Guide, November 2012
- Lexmark Common Criteria Installation Supplement and Administrator Guide, May 2013
- MX610 Series User's Guide, June 2012
- XC2100 Series User's Guide, September 2012
- MX710 Series User's Guide, May 2012
- MX810 Series User's Guide, May 2012
- MX410 and MX510 Series User's Guide, June 2012
- XM7100 Series User's Guide, September 2012

6.3 Life Cycle

- Lexmark Flaw Remediation, Version 1.1, April 25, 2013
- Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Configuration Item

List, Version 1.1, August 6, 2013

- Lexmark Configuration Management Plan, Version 1.1, April 29, 2013
- Lexmark Delivery, Version 1.1, April 29, 2013

7 IT Product Testing

Testing was completed on August 2, 2013 at the COACT CCTL in Columbia, Maryland and at Lexmark International, Inc. in Lexington, KY. COACT employees performed the tests.

7.1 Developer Testing

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

The evaluator selected to test two of the MFPs to verify the TOE meets the requirements identified in the Security Target. The evaluator tested the Lexmark MX811 and the combination of the Lexmark MX711dhe. As a result, the selected test sample represented the entire TOE configuration.

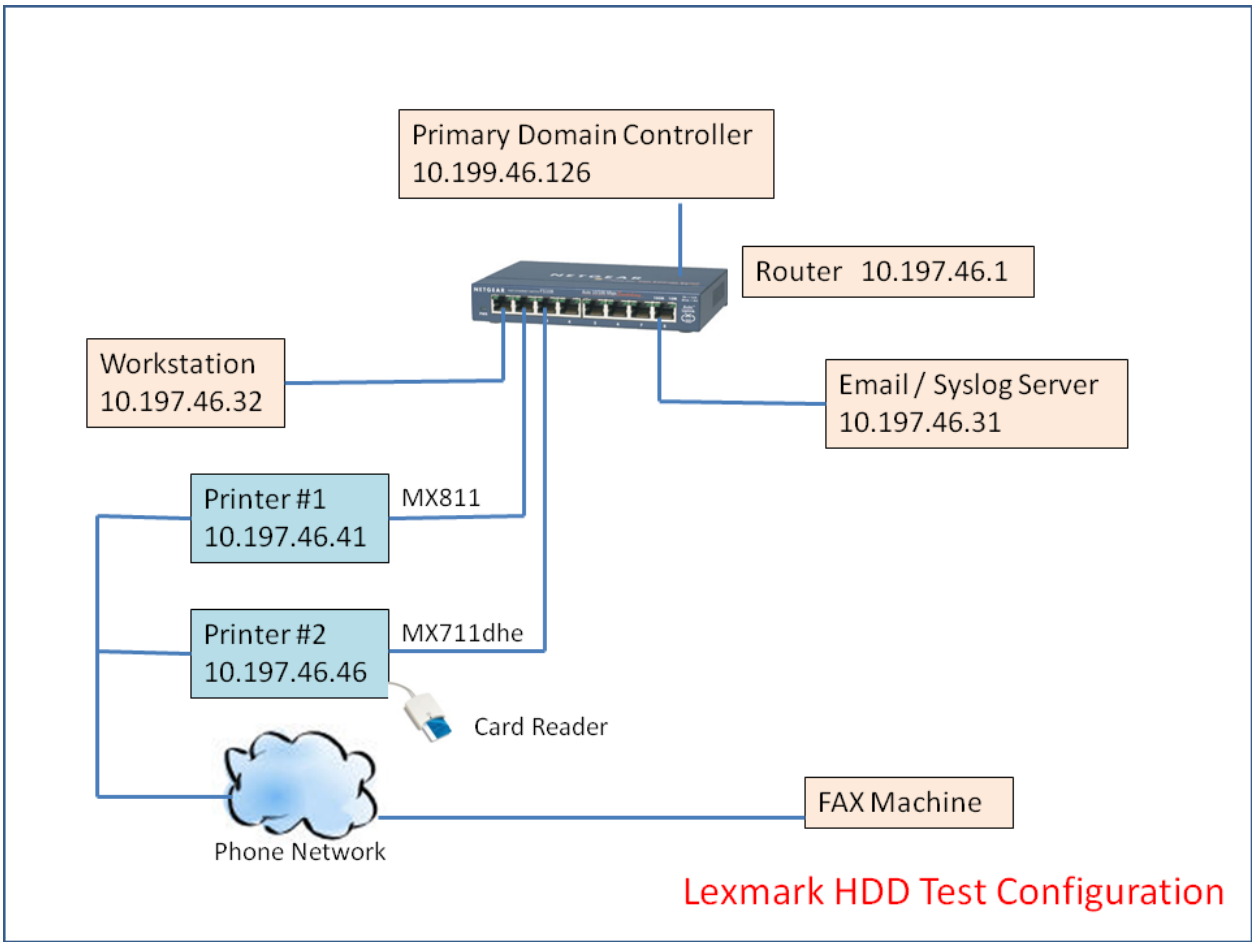

Figure 2: Test Configuration/Setup

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

Table 6: 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. This system is Windows XP configured in a virtual environment. IP Address = 10.197.46.32
AD Server	This system acts as the Primary Domain Controller for the network, providing Active Directory, Kerberos, GSSAPI, DNS, NTP, and PKI services. IP Address = 10.199.46.126
SMTP/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 diaplaying Syslog messages from Printer 1 and Printer 2. This is a virtual machine running Centos 5. IP Address = 10.197.46.31
Virtual Machine Host	The virtual machine host is using SYBIL to host the Syslog Server and the Workstation Browser. Wireshark is installed on this computer which will be used to monitor the test network. This virtual machine host is outside of the IPSec configuration. IP Address = 10.197.46.32
Attack PC	A network monitor able to analyze and display the traffic between Workstation and the MFPs and to launch other penetration tests. IP Address = 10,197.46.35
Printer 1	One instance of the Lexmark MX811 without a Smart Card reader. IP Address = 10.197.46.41
Printer 2	Second instance of the Lexmark MX711dhe with a Smart Card reader. IP Address = 10.197.46.46
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).

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 7: Workstation Requirements

Description	Test Configuration Specific Details
Authorized Users	“user1”

Table 8: Primary Domain Controller

Description	Test Configuration Specific Details
DNS Configuration	Entries for all active systems connected to IP Network
NTP Configuration	Acting as server No authentication required

Table 9: E-mail/Syslog Server

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

Table 10: Printer 1 Requirements

Description	Test Configuration Specific Details
Internal Account Groups	"Administrators" "Users" "Restricted" "Fax"
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" User "fax" as a member of "Fax"
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" "Fax_Users" with "Internal_Accounts_Building_Block" for authentication and authorization and group "Fax"
User Functions Enabled	Fax, Email, Copy
Function Access Controls	E-mail: Authorized_Users Fax: Fax_Users Solution 1: Authorized_Users Copy: 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 Email/Syslog Server 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

Located below are the configuration settings for the second printer in the testing lab's test configuration. Since the vendor did not test the functionality of the CAC Card Access Control, the lab has implemented an independent test to exercise the functionality of this feature.

Table 11: 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

Description	Test Configuration Specific Details
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 12: Network Monitor

Description	Test Configuration Specific Details
Penetration and Attack Tools	Windows XP Professional SP3 Internet Explorer (Including all updates and patches) WinZip 10 ZENMAP GUI 5.21 Nmap 5.21 SnagIt 8 WireShark 1.6.2

Table 13: Test Assumptions

Assumption	Definition
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.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.

All other assumptions associated with each test will be identified at the beginning of each set of test procedures.

7.2 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 with Hard Drives Test Report August 5, 2013, Document No. E2-0313-008.

7.3 Evaluation Team 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.

7.4 Evaluator Penetration Tests

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

A) http://osvdb.org/

B) http://secunia.com/

C) http://web.nvd.nist.gov

D) http://www.securityfocus.com/

E) http://www.lexmark.com

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

A) Lexmark

B) Lexmark Printer

C) Multi Function Printer

D) Lexmark MFP

E) MFD

The evaluator selected the search key words based upon the following criteria. The terms "Multi Function Printer", "MFP", and "MFD" were used to identify vulnerabilities related to printers. The searches that contained the keywords "Lexmark" were selected to further refine the search directly related to the TOE.

7.5 Test Results

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

The end result of the evaluator penetration tests did not reveal any vulnerabilities.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is any one of the Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers including any combination of the following items connected to the TOE:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.
2. A telephone line for fax capability.
3. IT systems that submit print jobs to the MFP via the network using standard print protocols.
4. IT systems that send and/or receive faxes via the telephone line.
5. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
6. LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
7. Card reader and cards to support Smart Card 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:
    a. Omnikey 3121 SmartCard Reader,
    b. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),
    c. SCM SCR 331,
    d. SCM SCR 3310v2.

:

9 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 with Hard Drives Test Report, August 5, 2013, Document No. E2-0313-008.

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

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Lexmark Multifunction Printers with Hard Drives meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- There are several configuration parameters contained in the ST and highlighted in Section 4.4 above that must be followed to ensure the product is operated in the secure manner required of the evaluated configuration. Failure to follow these guidelines will negate the assurances provided by the evaluation.
- Audit records of TOE activity are exported to an external entity. Administrators of the product must ensure that there is sufficient storage for these records. In addition, the external audit storage must be protected from unauthorized access and modification or deletion of the audit records.

11 Security Target

The Security Target is identified as the Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Security Target, version 1.10, January 8, 2014. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2.

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 Orgaization
IT Information Technology
KDC Key Distribution Center
LAN Local Area Network
LDAP Lightweight Directory Access Protocol
MB MegaByte
MFD Multi-Finction Device
MFP Multi-Function Printer
NTP Network Time Protocol
OSP Organizational Security Policy
PCL Product Compliant List
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 Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL). An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

Conformance. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

Evaluation. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation Evidence. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Feature. Part of a product that is either included with the product or can be ordered separately.

Target of Evaluation (TOE). A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

Validation. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

Validation Body. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R4, September 2012.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R4, September 2012.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R4, September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R4, September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.

[6] COACT Café Lab. Lexmark Multi-Function Printers with Hard Drives Test Report, August 5, 2013, Document No. E2-0313-008.

[7] COACT Café Lab. *Lexmark Hard Drive Printers Evaluation Technical Report*, August 15, 2013, Document No. E2-0513-008.

[8] Lexmark MX511h, MX611h, MX710h, MX711h, MX810, MX811, MX812, XM7155, XM7163, XM7170, CX510h and XC2132 Multi-Function Printers Security Target, Version 1.10, January 8, 2014.