Lexmark™ Crypto-Module

FIRMWARE VERSION 2.10

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 1.5

July 2015

Table of Contents

Revision History

Version	Date	Change
1.0	June 10, 2014	Prerelease Document
1.1	July 17, 2014	Initial Document
1.2	September 2014	Added MS911 series printers and corrected typos. Added input and output columns to Table 8.
1.3	November 2014	Testing laboratory changes
1.31	November 2014	Correction to Table 8 and Self-Tests
1.4	January 2015	Revised and added printers to tables 2 and 3
1.5	July 2015	CMVP comment changes

Introduction

Purpose

This is a non-proprietary Security Policy describing how the Lexmark™ Version 2.10 Crypto Module meets the requirements of FIPS 140-2. This Security Policy describes the method by which the module may be configured to meet the FIPS requirements for secure operation. This Security Policy was prepared as part of a Level 1 FIPS 140-2 validation.

References

Information on Lexmark™ products may be found at (http://www.lexmark.com/en_US/)

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Modules) describes the U.S. Government requirements for cryptographic modules. Information about the Cryptographic Module Validation Program (CMVP) is available at (http://csrc.nist.gov/groups/STM/cmvp/)

This document is but one of many that are required in a FIPS 140-2 Submission Package, which includes proprietary vendor evidence. With the exception of this non-Proprietary Security Policy, all other documentation pertinent to this validation effort is only available from Lexmark™ International under appropriate non-disclosure agreements.

Lexmark™ Crypto Module v2.10

Overview

The Lexmark™ Crypto Module v2.10 is a firmware option for Lexmark™ and Dell® Multi-Function Printers that permit the transfer, storage and printing of encrypted print jobs. Using the Lexmark™ Crypto Module v2.10, a printer is capable of encrypting and decrypting data input to and output from the module crypto kernel using the AES (FIPS 197) encryption algorithm.

Module Specification

The module is a multi-chip standalone cryptographic module as defined by FIPS PUB 140-2.

Module Level Specification

The Lexmark™ Crypto Module v2.10 meets FIPS PUB 140-2 overall Level 1 as shown in Table 3:

FIPS 140-2 Section	Section Title	Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of other Attacks	N/A

Table 1: FIPS 140-2 Security Level by Section

Supported Devices

The Lexmark™ Crypto Module v2.10 is available for the following Lexmark™ and Dell® brand printers. No claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate

Single Function Devices (no scanner)

Product	Type/Model	FCC	ISO/IEC 17050-1 and EN 17050-1
Lexmark MS310d Lexmark MS310dn	4514-220 4514-230	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS312dn	4514-330	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS315dn Lexmark MS415dn Lexmark M1140+	4514-335 4514-530 4514-539	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS410d Lexmark MS410dn Lexmark M1140	4514-420 4514-430 4514-439	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Dell 2360d Dell 2360dn	4514-42d 4514-43d	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS510dn Lexmark M1145	4514-630 4514-639	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009

Lexmark MS610dn Lexmark MS610dtn	4514-635 4514-635	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Dell 3460dn	4514-6d5	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS610de Lexmark MS610dte Lexmark M3150	4514-646 4514-646 4514-649	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS710dn Lexmark MS711dn	4063-832 4063-835	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS810n Lexmark MS810dn Lexmark MS810dtn	4063-210 4063-230 4063-230	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS811n Lexmark MS811dn Lexmark MS811dtn	4063-410 4063-430 4063-430	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS812dn Lexmark MS812dtn	4063-630 4063-630	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Dell 5460dn	4063-43d	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009

Lexmark MS810de Lexmark M5155	4063-23E 4063-29E	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS811de Lexmark M5163	4063-43E 4063-49E	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS812de Lexmark M5170	4063-63E 4063-69E	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MS911de	4021-230	Class A	EN 55024:2010 EN 55022:2010 +AC:2011 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark CS310n Lexmark CS310dn	5027-210 5027-230	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark CS410n Lexmark CS410dn Lexmark CS410dtn	5027-410 5027-430 5027-430	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark CS510e Lexmark CS510de Lexmark CS510dte	5027-610 5027-630 5027-630	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009

Table 2: Single Function Devices

Multi-Function Devices

Product	Type/Model	FCC	ISO/IEC 17050-1 and EN 17050-1
Lexmark MX310dn	7015-270	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX410de Lexmark XM1140	7015-470 7015-479	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX510de Lexmark MX511de Lexmark MX511dte Lexmark MX511dhe Lexmark XM1145	7015-630 7015-670 7015-670 7015-675 7015-679	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX610de Lexmark MX611de Lexmark MX611dfe Lexmark MX611dhe Lexmark XM3150	7016-630 7016-670 7016-675 7016-675 7016-679	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Dell 3465dn Dell 3465dnf	7016-63d 7016-67d	Class B	EN 55024:2010 EN 55022:2010 + AC:2011 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX710de Lexmark MX710dhe Lexmark XM5163	7463-036 7463-037 7463-096	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX711de Lexmark MX711dhe Lexmark MX711dthe Lexmark XM5170	7463-236 7463-237 7463-237 7463-296	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Dell 5465dnf	7463-2d7	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX810de Lexmark MX810dfe Lexmark MX810dme Lexmark MX810dte Lexmark MX810dtfe Lexmark MX810dtme Lexmark MX810dxe Lexmark MX810dxfe Lexmark MX810dxme Lexmark MX810dpe	7463-436 7463-436 7463-436 7463-436 7463-436 7463-436 7463-436 7463-436 7463-436 7463-436	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009

Lexmark MX810dtpe Lexmark MX810dxpe Lexmark XM7155 Lexmark XM7155x	7463-436 7463-436 7463-496 7463-496		
Lexmark MX811de Lexmark MX811dfe Lexmark MX811dme Lexmark MX811dte Lexmark MX811dtfe Lexmark MX811dtme Lexmark MX811dxe Lexmark MX811dxfe Lexmark MX811dxme Lexmark MX811dpe Lexmark MX811dtpe Lexmark MX811dxpe Lexmark XM7163 Lexmark XM7163x	7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-636 7463-696 7463-696	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX812de Lexmark MX812dfe Lexmark MX812dme Lexmark MX812dte Lexmark MX812dtfe Lexmark MX812dtme Lexmark MX812dxe Lexmark MX812dxfe Lexmark MX812dxme Lexmark MX812dpe Lexmark MX812dtpe Lexmark MX812dxpe Lexmark XM7170 Lexmark XM7170x	7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-836 7463-896 7463-896	Class A	EN 55024:2010 EN 55022:2010 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark MX910de Lexmark MX911dte Lexmark MX912dxe Lexmark XM9145 Lexmark XM9155 Lexmark XM9165	7421-036 7421-236 7421-436 7421-039 7421-239 7421-439	Class A	EN 55024:2010 EN 55022:2010 +AC:2011 (Class A) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark CX310n Lexmark CX311dn	7527-211 7527-231	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009
Lexmark CX410e Lexmark CX410de Lexmark CX410dte	7527-415 7527-436 7527-436	Class B	EN 55024:2010 EN 55022:2010 (Class B) EN 61000-3-3:2008 EN 61000-3-2:2006 + A1:2009 +A2:2009

Lexmark CX510de	7527-636	Class B	EN 55024:2010
Lexmark CX510dhe	7527-637		EN 55022:2010 (Class B)
Lexmark CX510dthe	7527-637		EN 61000-3-3:2008
Lexmark XC2132	7527-697		EN 61000-3-2:2006 + A1:2009 +A2:2009

Table 3: Multi-Function Devices

Approved Algorithms

The Approved User algorithms are listed in Table 4; the Approved Kernel algorithms in Table 5. For details see CAVP validation list at: http://csrc.nist.gov/groups/STM/cavp/validation.html

Algorithm	Usage	Certificate #
HMAC: HMAC-SHA-1, HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Integrity check	1479
SHS: FIPS 180-3 SHA-1 (BYTE only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	Secure hashing	2049

Table 4: Approved User Algorithms

Algorithm	Description	Certificate #
AES: CBC FIPS 197	Kernel Encryption/Decryption using 128-, 192-, and 256-bit keys	2380
SHS: SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	Secure Hashing	2050
HMAC: HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Kernel Services	1480

Table 5: Approved Kernel Algorithms

Cryptographic Boundary

Physical Cryptographic Boundary

The physical cryptographic boundary is defined as the printer case perimeter.

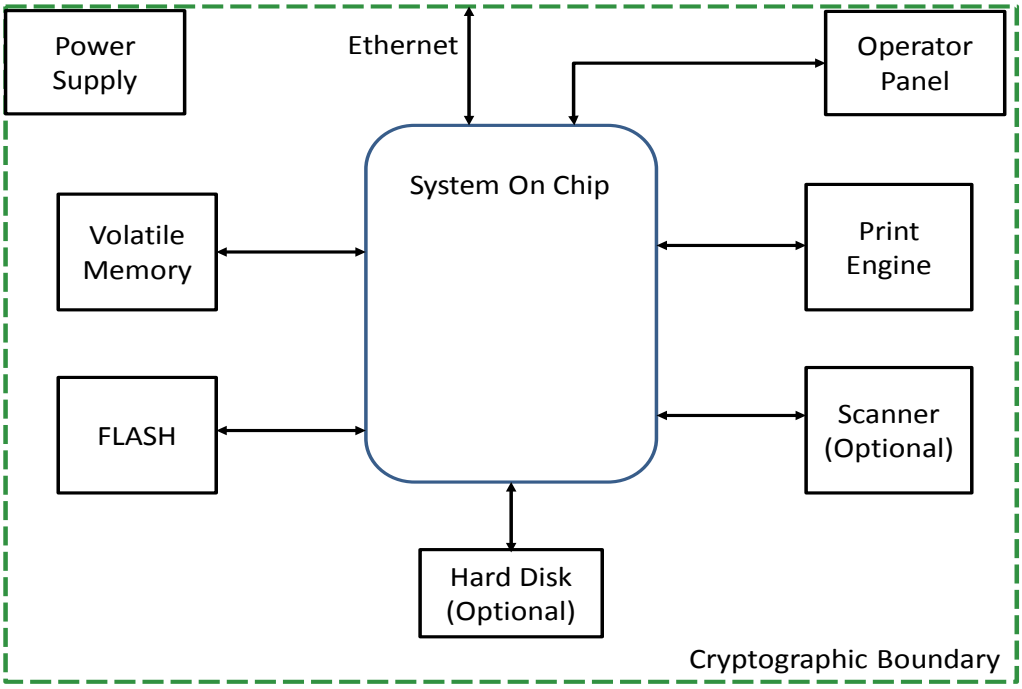

Figure 1: Cryptographic Boundary

Logical Cryptographic Boundary

The logical boundary is defined by the processor, memory and firmware specific to the cryptographic module. The logical cryptographic boundary consists of the FIPSCHECK interface and the CRYPTO KERNEL

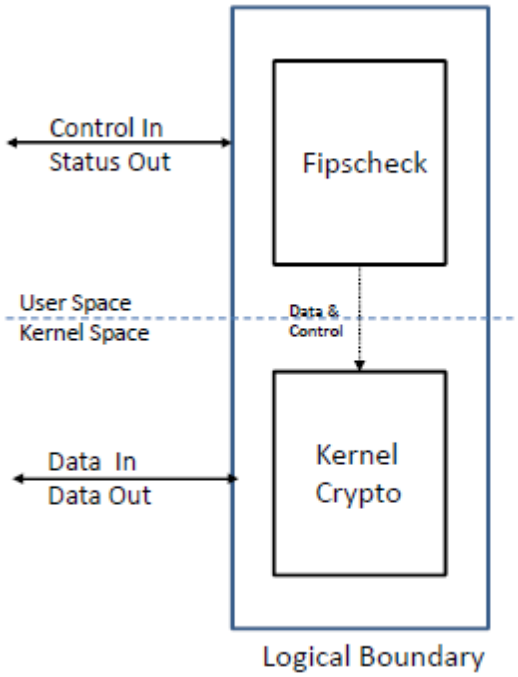

Figure 2: Logical Boundary

Module Interfaces

The crypto module's physical interfaces consist of the physical printer ports, including USB port, network port, paper exit port, feeder port, and LCD display. Encrypted data coming to the printer enters via the network wired or wireless (optional) or USB port as selected by the crypto-officer.

Control data is input via the physical ports, but is logically distinct from the input data. Data input and output includes enciphered data which exit via the logical boundaries to the network ports. Status outputs are sent via the network and are stored in a log file. Selected status is also available via the LCD display.

Data in and out of the logical module is via API calls.

Ports and Interfaces Table

FIPS Logical Interface	Module Physical Interface
Data Input	10/100/1000 Ethernet Port 802.11b/g/n Wireless Port* USB 2.0 port IEEE 1284*
Data Output	10/100/1000 Ethernet Port 802.11b/g/n Wireless Port* USB 2.0 port IEEE 1284*
Control Input	10/100/1000 Ethernet Port 802.11b/g/n Wireless Port* USB 2.0 port IEEE 1284* Power Switch Multipurpose Feeder Operator Panel
Status Output	10/100/1000 Ethernet Port 802.11b/g/n Wireless Port* USB 2.0 port IEEE 1284* Operator Panel LCD Paper Exit Port
Power Input	120 VAC Power Connector

Table 6: Ports and Interfaces * Optional feature

Identification and Authentication Policy

Roles and Services

The Crypto Module supports two roles; the Crypto-Officer and User. A maintenance role is not supported. Roles are assumed implicitly by the printer operator. FIPS authentication methods are not supported.

Crypto-Officer Role

The Crypto-Officer configures and activates the printer, runs self-test, and show-status service. Status is available via the printer log and LCD.

User Role

The User operates the printer by executing print jobs.

Services

Role	Service	Description	Input	Output	CSP	Access to CSP
Crypto Officer	Activate	Power on the Device	Power switch	Result of activation	none	n/a
Crypto Officer	Deactivate	Power off the device	Power switch	Deactivated module	none	n/a
Crypto Officer	Self-Test	Activate the device	Command	Status output	Integrity Check Keys	Read
Crypto Officer	Key Zero	Wipe CSPs	Command	Status Output	AES key	Write
Crypto Officer	Show Status	View status Log	Command	Status Output	None	n/a
User	Load Key		Command	Status Output	AES key	Write
User	Encrypt		Command	Status Output	AES key	Read
User	Decrypt		Command	Status Output	AES key	Read
User	Hash		Command	Status Output	HMAC key	Read

Table 7: Services

Crypto Officer Guidance

The crypto officer is responsible for configuring and monitoring the module. The Crypto Officer is responsible for confirming the module is factory installed by printing a Menu Page and confirming that **Crypto Module** and appropriate version number is displayed under the **Device Information** section of the Menu Page.

Key Zeroization: Key zeroization is a single write of zeroes over volatile memory. The module has no non-volatile key storage; keys are zeroized automatically after each use.

Authentication

Lexmark™ does not claim FIPS authentication validation for this module. Neither Users nor Crypto-Officers are authenticated.

Physical Security Policy

The Lexmark™ Crypto-Module runs on Lexmark™ and Dell® printers. The printers are commercial units made of production grade components. The printers are enclosed in a strong plastic and metal case which surrounds all hardware and firmware components.

Access Control

Access to module internals, including keys and other critical security parameters, is not available. Printers can only be physically accessed by users to retrieve print jobs.

Physical Control

Each physical unit is identified by a manufacturer generated serial number. Units are shipped using commercial methods and tracked to the destination where a receipt is obtained upon delivery. Control then shifts to the using organization.

Operational Environment

The operational environment is non-modifiable; there is no direct access to the OS by users outside the module. There is no method by which users may load third party firmware or software applications on the module. The operating system is Lexmark™ Linux version 3.0.0 which is configured in single user mode by default. The operating system is used as an embedded OS within the printers, and there is no direct access to the OS provided.

Both printer and algorithms were tested using the operating system listed above. The model MX811de printer was used for a CMVP testing platform.

Key Management

Module keys are not internally generated. Keys are either hardcoded into the firmware or externally loaded into the module by the appropriate API. Key is never exported (output) from the module.

Algorithms

Key or CSP	Type	Input	Generation	Storage	Use	Zeroize
AES	Session Key 128, 192, 256 bit	Plain Text	External	PT Volatile memory	Encrypt/Decrypt Data	At session close by writing zeros over memory
Integrity Check	256 bit HMAC	N/A	Hardcoded	PT Volatile memory	Self-test	Writing zeroes over FLASH image
HMAC	224, 256, 348 512 bit	Plain Text	External	PT Volatile memory	Secure hashing	At session close by writing zeros over memory

Table 8: Keys and CSP

Critical Security Parameters

1. HMAC Key for integrity check
2. AES encryption/decryption Key
3. HMAC Key for secure hashing

Key Zeroization

Keys are not stored in non-volatile memory. At session termination keys are destroyed by writing zeroes over the memory addresses.

Wiping printer memory

Erase individual settings, device and network settings, security settings, and embedded solutions by following these steps:

Turn off the printer.

Hold down **2** and **6** on the keypad while turning the printer on. Release the buttons only when the screen with the progress bar appears.

The printer performs a power-on sequence, and then the Configuration menu appears. When the printer is fully turned on, a list of functions appears on the printer display.

Press the up or down arrow button until **Wipe All Settings** appears.

The printer will restart several times during this process. Note: **Wipe All Settings** securely removes device settings, solutions, jobs, and passwords from the printer memory.

Self-Test

At each power up or on demand by the crypto-officer, the module runs the power on self-test suite. Results are reported to the status output (LCD) and the device log. Should any self-tests fail; the module outputs an error indicator and enters the error state.

Power-up Tests

The user-space and kernel space portions of the module perform their own KAT tests, independent of each other.

Cryptographic Algorithm KAT:

User Space: HMAC using SHA-1, SHA-224, SHA-256, SHA-384 & SHA-512,.

Kernel Space: AES;

HMAC using the following:

SHA-224

SHA-256

SHA-384

SHA-512

Software/Firmware integrity: HMAC SHA 256

Conditional Tests

None

EMI/EMC

The module conforms to EMI/EMC requirements specified by Section 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (for business use) or Class B (for home use); specified by printer model in Tables 1 and 2.

Design Assurance

Configuration Management

Source code and associated documentation files are managed and recorded using MLS. MLS is an in-house configuration management system that provides a version control that stores multiple revisions of the same file with a revision history and older versions are always accessible.

Additionally, Subversion (SVN) is used to provide version control for the module's FIPS documentation. This software provides access control, versioning and logging.

Mitigation of other attacks

The Crypto-Module does not mitigate against any other attacks.

Operation in FIPS mode

The module operates in FIPS mode by default. No other operational mode is available.

Acronymns

AES	Advanced Encryption Standard
API	Application Programmer Interface
CBC	Cipher Block Chaining
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FLASH	An electronic erasable non-volatile computer storage medium
HMAC	Hash-based Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
KAT	Known Answer Test
LCD	Liquid Crystal Display
MLS	Lexmark™ Configuration Control Management System
NIST	National Institute of Standards and Technology
OS	Operating System
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SVN	Lexmark™ Subversion Control System
USB	Universal Serial Bus