# Lexmark PrintCryption™

(Firmware Versions 1.3.2a  and 1.3.2i)

## FIPS 140-2 Non-Proprietary Security Policy

**Level 1 Validation**
**Version 1.15**

**May, 2010**

# Table of Contents

# Introduction

## *Purpose*

This is a non-proprietary Cryptographic Module Security Policy for the Lexmark PrintCryption$^{TM}$ from Lexmark International Inc. This Security Policy describes how the Lexmark PrintCryption$^{TM}$ meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The Lexmark PrintCryption$^{TM}$ is referred to in this document as PrintCryption, PrintCryption module, cryptographic module, firmware module, or module.

## *References*

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Lexmark International website (http://www.lexmark.com) contains information on the full line of products from Lexmark International.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

## *Document Organization*

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Lexmark and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Lexmark International.

# LEXMARK PRINTCRYPTION™

## *Overview*

The Lexmark PrintCryption™ is an option for the Lexmark printers that enable the transfer and printing of encrypted print jobs. This new Lexmark technology offers a level of security that is the first of its kind in the printing industry. With the PrintCryption module installed, the printer is capable of decrypting print jobs encrypted with the AES (FIPS 197) algorithm. The Lexmark PrintCryption™ analyses the encrypted data stream, determines if the correct key was used to encrypt the data, decrypts the data and allows the confidential document to be printed. This new level of printing security is ideal for industries that commonly handle sensitive or personal information, such as financial institutions, government agencies, and healthcare organizations.

## *Module Specification*

The version 1.3.2i PrintCryption™ module is a firmware module composed of three binaries (aessd, dkmd & libcl.so) on the IBM750CL processor platform. The version 1.3.2a PrintCryption™ module is composed of two binaries (aessd & dkmd) on the ARM9 processor platform.  The module is enabled in Lexmark printers using a Downloaded Emulator Card (DLE), a PCI interface PCB board that plugs into the printer which contains an activation code. The DLE card is shown in Figure 1.

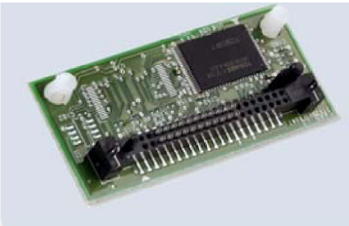


**Figure 1 - Optional Firmware Card**

Per FIPS PUB 140-2, PrintCryption™  is classified as multi-chip standalone cryptographic module. The module meets overall level 1 FIPS 140-2 requirements, as detailed in Table 2.

| Printer Model | Processor | Part Number |
|---|---|---|
| E460 | ARM9 | P/N 34S0700 |
| T650 | IBM 750CL | P/N 30G0100 |
| T652 | IBM 750CL | P/N 30G0210 |
| T654 | IBM 750CL | P/N 30G0310 |
| C734 | IBM 750CL | P/N 25C0350 |
| C736 | IBM 750CL | P/N 25A0450 |
| W850 | IBM 750CL | P/N 19Z0300 |
| X463 | ARM9 | P/N 13C1100 |
| X464 | ARM9 | P/N 13C1101 |
| X466 | ARM9 | P/N 13C1102 |
| X651 | IBM 750CL | P/N 16M1255 |
| X652 | IBM 750CL | P/N 16M1260 |
| X654 | IBM 750CL | P/N 16M1265 |
| X656 | IBM 750CL | P/N 16M1797 |
| X658 | IBM 750CL | P/N 16M1301 |
| X734 | IBM 750CL | P/N MS00300 |
| X736 | IBM 750CL | P/N MS00301 |
| X738 | IBM 750CL | P/N MS00321 |
| X860 | IBM 750CL | P/N 19Z0100 |
| X862 | IBM 750CL | P/N 19Z0101 |
| X864 | IBM 750CL | P/N 19Z0102 |

**Table 1 – Printers that Maintain the PrintCryption FIPS 140-2 Validation (Option P/N 30G0829):**

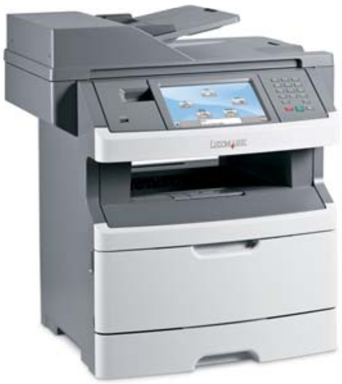


**Figure 2 - X463 with PrintCryption 1.3.2a**

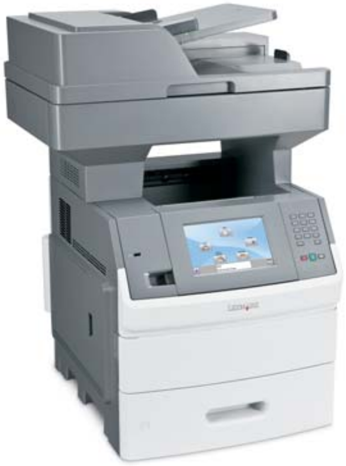


**Figure 3 - X651 with PrintCryption 1.3.2i**

Operating System: Lexmark proprietary ver. 2.6 based on the Linux operating system.

| Section | Section Title | 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 2 – Security Level per FIPS 140-2 Section**

Logically, the cryptographic boundary is composed of three binaries and is evaluated for use on Lexmark printers that are running Linux operating system. Once the PrintCryption firmware is activated in the printer, the printer must use this firmware. The cryptographic module cannot be bypassed. Functionality is then controlled by the PrintCryption firmware.

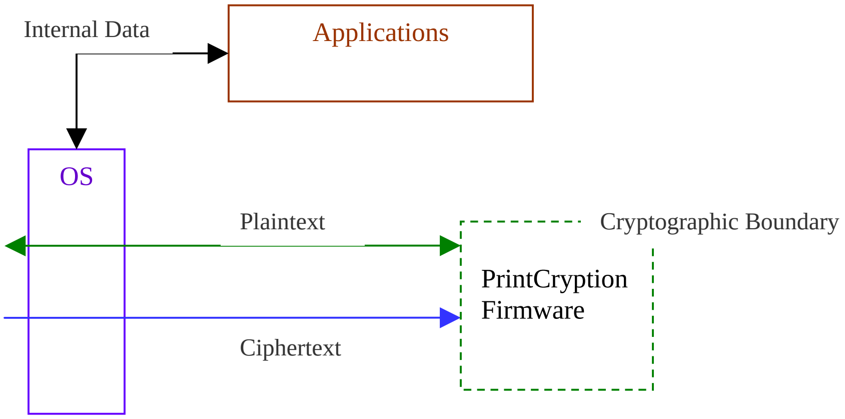


**Figure 4 - Logical Cryptographic Boundary**

The PrintCryption module is evaluated for running on number of Lexmark printers including mono-color printers (E460, T650, T652, T654 and W850), Color printers (C734 and C736), mono-color MFP printers (X463, X464, X466, X651, X652, X654, X656, X658, X860, X862 and X864) and color MFP printers (X734, X736 and X738). The module’s physical cryptographic boundary is the metal and plastic enclosure of the printer.

Within the physical cryptographic boundary are the following components:

- A CPU which executes the module binaries
- FLASH memory storage which stores the module binaries
- Volatile memory consisting of RAM
- A custom ASIC which contains support circuitry including: RAM controller, PCI buss interface, IO port interfaces and print engine interface circuits.
- An option slot containing the PrintCryption DLE card connected to the PCI bus
- The print engine consisting of various electronics and mechanisms that constitute the print device, sensors, and operator panel

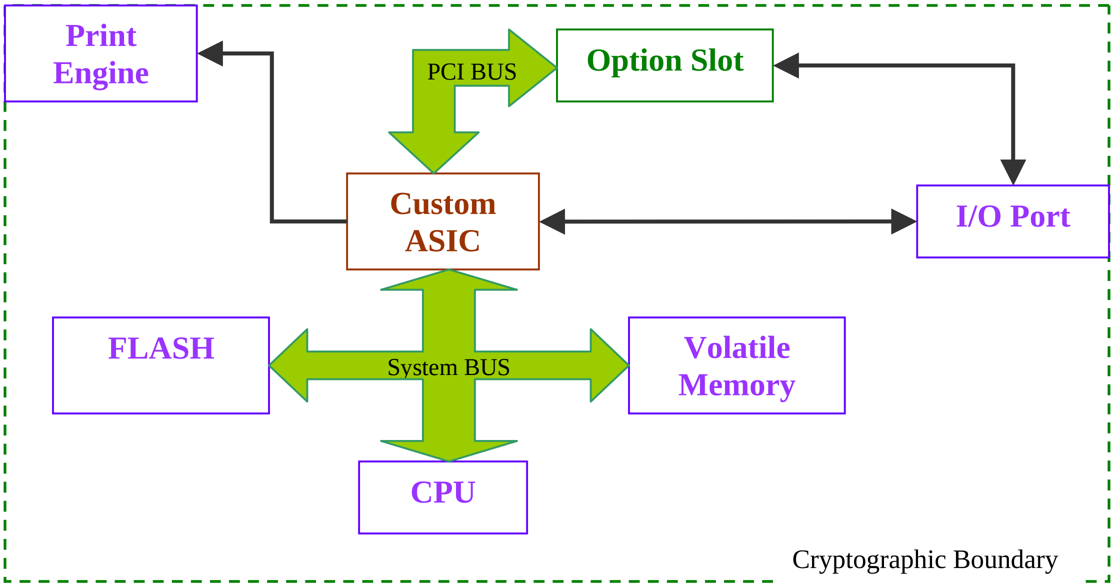


**Figure 5 - Physical Cryptographic Boundary**

### *Module Interfaces*

The cryptographic module’s physical ports are composed of the physical ports provided by the hardware platforms listed above. These printer ports include the network port, optional parallel port, USB port, paper exit port, multipurpose feeder, LED, and LCD display.

Since all of the module’s services are server processes, the logical interfaces of the module are network port and API calls, which provide the only means of accessing the module’s services. Data inputs are service requests on the TCP ports. Control inputs are also data at TCP/IP port, however they are logically distinct from Data input and controls how the function is executed. The data output from the module includes X.509 certificate and deciphered data, which exit through the network port and an internal API, respectively. The status outputs of the module are sent via network and stored in log file.

All of these physical ports are separated into logical interfaces defined by FIPS 140-2, as described in the following table.

| Logical Interface of the Module | Module Physical Port | FIPS 140-2 Logical Interface |
|---|---|---|
| Network Port | Network (Ethernet 10/100) Port<br>USB Port<br>Parallel Port (optional) | Data Input Interface |
| Network Port<br>Internal API | Network (Ethernet 10/100) Port<br>Paper Exit Port | Data Output Interface |
| Network Port | Operator Panel<br>Network (Ethernet 10/100) Port<br>USB Port<br>Parallel Port (optional)<br>Multipurpose/envelope Feeder<br>Power Switch | Control Input Interface |
| Network Port<br>Log File | LED<br>LCD Display<br>Network (Ethernet 10/100) Port<br>USB Port<br>Parallel Port (Optional)<br>Paper Exit Port | Status Output Interface |
| Not Applicable | Power Plug<br>Power Connector | Power Interface |

**Table 3 – FIPS 140-2 Logical Interfaces**

## *Roles and Services*

The module supports two roles, a Crypto Officer role and a User role, and an operator on the module implicitly assumes one of the roles. Descriptions and responsibilities for the two roles are described below.

### *Crypto Officer Role*

The Crypto Officer activates and deactivates the PrintCryption module by installing and removing the DLE card. The Crypto Officer is also responsible for Run Self Tests and Show Status services

| Service | Description | Input | Output | CSP | Type of Access to CSP |
|---|---|---|---|---|---|
| Activate | Assemble the printer and insert the DLE card to activate the PrintCryption module; Install printer driver on host PC | Command | Result of activation | None | -- |
| Deactivate | Remove the DLE card to deactivate the PrintCryption module | Command | Deactivated module | None | -- |
| Run Self-Test | Perform the self-test on demand | Command | Status output | Integrity Check Key | Read |
| Show Status | Call a show status from the printer status | Command | Status output | None | -- |

| Service | Description | Input | Output | CSP | Type of Access to CSP |
|---|---|---|---|---|---|
| | menu (HTTP) which has an LPC log page | | | | |

**Table 4 – Crypto Officer Services, Descriptions, CSPs**

*User Role*

Users utilize the cryptographic functionalities of the PrintCryption, and they communicate with the module via network port only.

Service descriptions and inputs/outputs are listed in the following table:

| Service | Description | Input | Output | CSP | Type of Access to CSP |
|---|---|---|---|---|---|
| Public Key request | Users request for printers public key. The module generates a key pair if needed | Public Key Request (PKR) at network port 9150. | X.509 certificate | RSA public key<br>RNG seed | Read/Write<br>Read |
| Secure Printing | AES encrypted printing program; Decrypts and prints the print job data using the supplied AES Session key | Encrypted print job at TCP/IP port 9152. | Status output | AES session key<br>RSA private key | Read/Write<br>Read |

**Table 5 – User Services, Descriptions, Inputs and Outputs**

## *Physical Security*

In FIPS terminology, the firmware module is defined as a multi-chip standalone cryptographic module. The module runs on Lexmark printers listed in *Module Specification* section. The printers are made of all production-grade components and are enclosed in a strong plastic and steel case, which surrounds all of the module's internal components, including all hardware and firmware.

The cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

## *Operational Environment*

The operational environment is non-modifiable and thus not applicable for this firmware module. The PrintCryption module runs on the Lexmark Linux v2.6 OS, and configured for single-user mode by default. The operating system is used as an embedded OS within the Lexmark printers, and there is no direct access to the OS provided.

## *Cryptographic Key Management*

The module implements the following FIPS-Approved algorithms.

| Algorithm | IBM750CL Certificate | ARM9 Certificate |
|---|---|---|
| AES ECB, CBC mode decryption – FIPS 197 | Certificate #1209 | Certificate #1208 |
| Deterministic Random Number Generator (RNG) – Appendix A.2.4 of ANSI X9.31 | Certificate #670 | Certificate #669 |
| HMAC – FIPS 198 | Certificate #704 | Certificate #703 |
| RSA (sign/verify) – PKCS#1.5 | Certificate #579 | Certificate #578 |
| SHS– FIPS 180-2 | Certificate #1112 | Certificate #1111 |

**Table 6 – FIPS-Approved Algorithms**

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementation:

- RSA Key Wrapping (PKCS #1): Key establishment method uses a 1024-bit key length providing 80-bits of security.

The module supports the following critical security parameters:

| Key or CSP | Key type | Generation | Storage | Use |
|---|---|---|---|---|
| AES Session Key | 128, 192, 256 bits AES key | Externally generated. Imported in encrypted form (RSA key transport) | Held in volatile memory in plaintext. Zeroized after the session is closed. | Decrypts input data for printing |
| RSA Public Key | 1024 bit RSA public key (80-bits of security) | Internally generated according to FIPS PUB 186-3 and IG A.6 | Stored on flash in plaintext. Zeroized by overwriting the flash image. | Key transport |
| RSA Private Key | 1024 bit RSA private key (80-bits of security) | Internally generated according to FIPS PUB 186-3 and IG A.6 | Stored on flash in plaintext. Zeroized by overwriting the flash image. | Key transport |
| Integrity Check Keys | 168 bit HMAC keys | Externally generated, hard coded in the module | Stored on flash in plaintext. Zeroized by overwriting the flash image. | Firmware Integrity test |
| PRNG Seed | 64 bits | Internally generated from non-approved RNG | Held in volatile memory only in plaintext. Zeroized after the session is closed. | RNG |
| PRNG Seed Key | 168 bits with 128 bits of entropy | Internally generated from non-approved RNG | Held in volatile memory only in plaintext. Zeroized after the session is closed. | RNG |

**Table 7 - Listing of Key and Critical Security Parameters**

*Access Control Policy*

User functionalities have read/write access to the AES Session Key and RSA public key. AES Session key is used to decrypt the data for printing. RSA public key is used for AES Session key transport. Integrity Check Keys can be read by Crypto-Officer “Run Self-Test” service.

*Key Generation*

The module key is generated internally is 1024 bits RSA key pair using key generation techniques that meet IG A.6 and FIPS Pub 186-3. FIPS-Approved PRNG X9.31 Appendix A.2.4 is used to seed the RSA key generation mechanism. AES Session Key is generated outside of the module and imported via RSA key transport.

*Key Storage*

The AES Session Key is held in volatile memory only in plaintext. The RSA public key is stored in flash memory in an X.509 certificate in plaintext, and the RSA private key is stored flash memory in plaintext.

*Key Entry and Output*

All keys that are entered into (AES key) or output from (RSA certificate) the module are electronically entered or output. AES Session Key is entered into the module transported (encrypted) by RSA public key.

*Key Zerorization*

AES Session key is an ephemeral key which is zeroized after the connection is closed or by rebooting the module. The module provides no service to erase or discard the RSA key pair. The key pair is erased by overwriting the flash image with a new image.

### *Self-Tests*

The PrintCryption module runs power-up and conditional self-tests to verify that it is functioning properly. Power-up self-tests are performed during startup of the module. Module startup occurs every time a new network connection is established and the dkmd or aessd process starts. Conditional self-tests are executed whenever specific conditions are met.

**Firmware Integrity Check:** The module employs a firmware integrity test in the form of HMAC SHA-1.

**Cryptographic Algorithm Tests:** Known Answer Tests (KATs) are run at power-up for the following algorithms:

- AES KAT

- RSA Sign/Verify and Encrypt/Decrypt pair-wise consistency check
- SHA-1 KAT
- X9.31 RNG KAT

The module implements the following Conditional self-tests:

- Continuous RNG Test for X9.31 PRNG
- Continuous RNG Test for non-approved RNG
- RSA Sign/Verify and Encrypt/Decrypt pair-wise consistency check

If any of these self-tests fail, the module will output an error indicator and enter an error state. All self-test results are logged in the device's Self-Test Log. The log is available through the device's web interface. The log messages are formatted as follows:

```
LOG: (<number>) <date> <time> :[PASS|FAIL] --> <message>
```

Where <number> is a integer which uniquely identifies the test and executable, <date> is the date of the test, <time> is the time of the test, and <message> is one test specific strings listed below.

- <progran name> PRNG KAT Test
- ERROR: Cryptlib could not init
- <program name> Software Integrity Check: Passed.
- <program name> Software Integrity Check: Failed. Could not open Known Hash file.
- <program name> Software Integrity Check: Failed. Memory allacation error.
- <program name> Software Integrity Check: Failed. Known Hash read error.
- <program name> Software Integrity Check: Failed. Hash files do not match.
- <program name> Software Integrity Check: Failed. Could not generate HMAC.
- <program name> Software Integrity Check: Failed. Unknown error.
- <program name> AES-ECB/CBC KAT SELF TESTING
- <program name> RSA Pair-wise Consistency Test (sign/verify)
- <program name> RSA Pair-wise Consistency Test (encrypt/decrypt)
- CRNG Test when creating new RSA keys
- Conditional RSA Key Generation Sign/Verify Test
- Conditional RSA Key Generation Encrypt/Decrypt Test

Where <program name> is one of DKMD, AESSD, or CRYPTLIB.

### *Design Assurance*

Source code and associated documentation files are managed and recorded using the MLS. MLS is a version control system that stores multiple revisions of the same file with a revisionary history and older versions are always accessible.

Additionally, Subversion is used to provide configuration management for the firmware module's FIPS documentation. This software provides access control, versioning, and logging.

### *Mitigation of Other Attacks*

The PrintCryption module does not employ security mechanisms to mitigate specific attacks.

## OPERATION IN FIPS MODE

The PrintCryption meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

### *Initial Setup*

The DLE card containing PrintCryption activation code may be factory installed or user-installed. Lexmark provides an Installation sheet, a driver CD with publications, and license agreement for the module in the option kit.

Installation procedure of the module is as follows.

1. Print a menu settings page:

    a. Press **Menu** until **Utilities** menu appears, and then press **Select**.

    b. Press **Menu** until Print menu appears, and then press **Select** to print the page.

    Note: This Page is needed for later use.

    c. Configure the printer onto the TCP/IP network per installation requirements. If the printer is behind a firewall, it must allow IP ports 9150 and 9152 to pass through.

2. Turn off the printer and install the card. Please refer to the printer's documentation for further instructions on installing the card.

3. Turn the printer on.

    a. If the printer displays the message **41 – Unsupported Firmware Card**, then the installed card is not compatible for the printer. Turn off the printer and remove the card.

    b. If the printer displays the message **Resetting all of NVRAM** for longer than 45 seconds, turn off the printer and reinstall the card.

4. Print a menu settings page. If "Lexmark PrintCryption Card" is not listed under **Installed Features,** turn off the printer and repeat steps 2 and 3.

    ```
    To identify if the module is in FIPS mode the Menu Settings
    Page must list "Lexmark PrintCryption Card" otherwise the
    FIPS module is not being used."
    ```

5. Launch the CD to host PC to install the software application using **setup.exe** program. Please refer to the documents on the CD for further

instructions on installing the software. The setup executable, once launched, will:

a. Ask for confirmation of the End-User License Agreement.

b. Present a small README, which explains that after installation, the Crypto Officer can add a new port to their printer driver that will support Lexmark PrintCryption$^{TM}$.

   Note: Please refer to *Crypto Officer Guidance* section for more information.

c. Perform the installation, and stop and restart the print spooler.

6. Print a menu settings page. Compare these settings to those on the page printed in step 1.

7. Place the Option Added label on the printer next to the printer model and serial number label. Lexmark provides the **Option Added** label with the Installation guide.

### *Crypto Officer Guidance*

The Crypto Officer is responsible for activating, deactivating and monitoring the module. The DLE card comes in a static sensitive package. Upon receiving the PrintCryption DLE card, the Crypto Officer should check for any signs of tampering to the package, including a damaged seal or package.

The Crypto Officer may follow the installation sheet found in the option kit to install the PrintCryption DLE card. After the installation is complete, the Crypto Officer must print a Menu page and verify that **Lexmark PrintCryption Card** is displayed under the **Installed Features** section of the Menu Page.

The Crypto Officer must configure the printer onto the TCP/IP network per installation requirements. While installing the PrintCryption host software application on a PC, Crypto Officer must choose **port 9150** to communicate with the printer. It is recommended that Crypto Officer name the port “FIPS” to clearly distinguish the port that provides secured printing service.

### *User Guidance*

The user software is a separate module which is not covered by this validation. This section is provided for the convenience of the user.

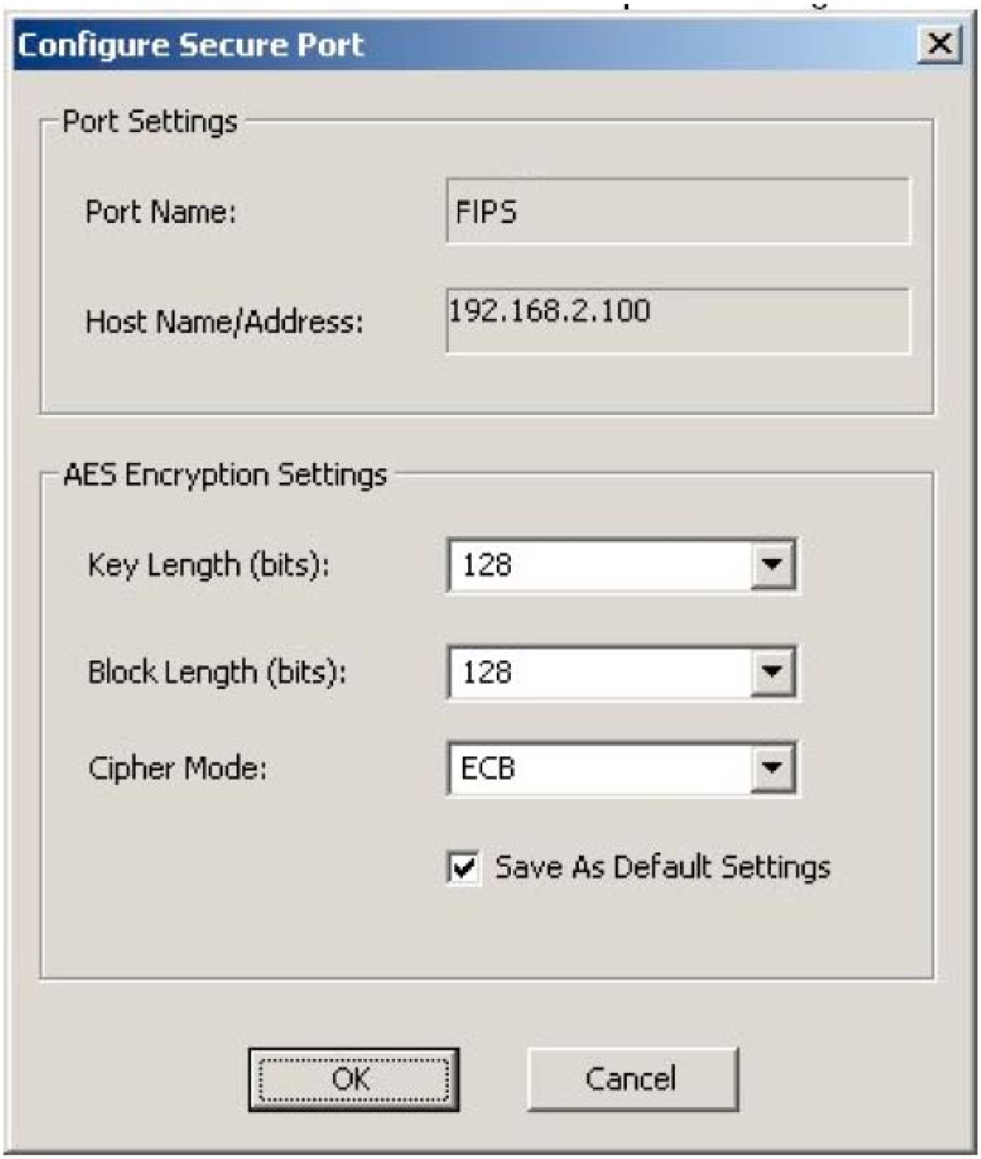
The User accesses the module printing functionality as a user over network. Although outside the boundary of the module, the User should be careful to use secured printing services as needed.

Uses can select the AES encryption key length, block length and mode using the printer property.

1. Open the printer folder, right click on the desired printer and select **Properties**.

2. Navigate to **Port** tab and press the **Configure Port** button to proceed.

3. **Configure Secure Port** dialog box will appear which enables Users to choose their options.



Configure Secure Port

Port Settings

Port Name: FIPS

Host Name/Address: 192.168.2.100

AES Encryption Settings

Key Length (bits): 128

Block Length (bits): 128

Cipher Mode: ECB

☑ Save As Default Settings

**Figure 6 - Configuring a Secure Port**

Users must choose the key size and block size approved in FIPS PUB 197 standard. FIPS approved key and block sizes, and mode of operation are as follows:

- Key Length: 128, 192, or 256 bit.
- Block Length: 128 bit. (only selection available)
- Cipher Mode: ECB (Electronic Code Book, or CBC (Cipher Block Chaining)).

Setup.exe also installs the Lexmark PrintCryption Utility (LPCU) program as part of the install session. The program can be invoked by -

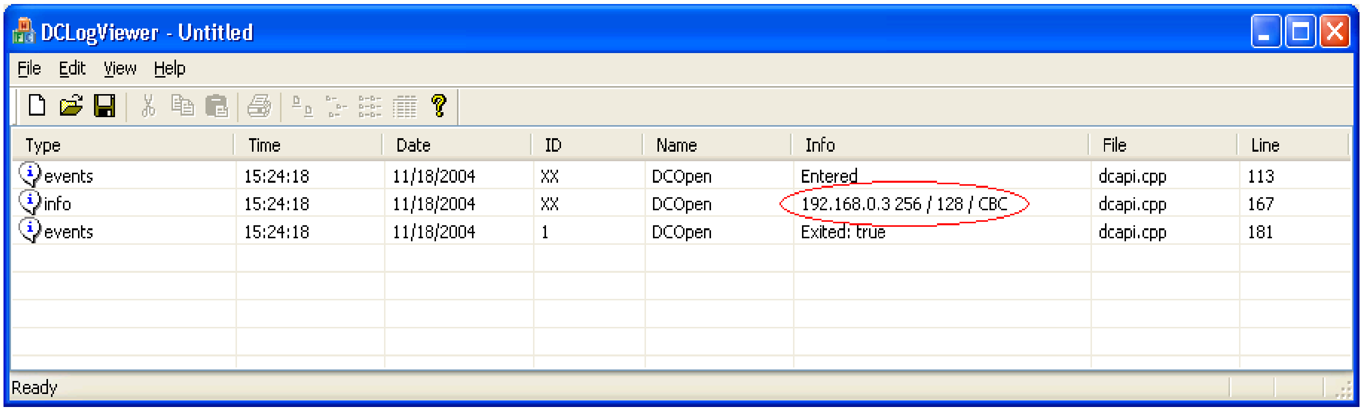
START → Programs → Lexmark → PrintCryption → PrintCryption Test Utility

The LPCU utility program can help Users to determine:

- The Lexmark PrintCryption Card is installed.
- The network path exists, even through a firewall, and when **ping** command does not work.
- The proper IP ports (9150 and 9152) are open.
- The printer is capable of returning an X.509 security certificate.
- The printer can successfully decode an encrypted packet.

Users also can view the communication to the printer via PrintCryption Log Viewer, installed during the installation session, which can be started by -

START → Programs → Lexmark → PrintCryption → PrintCryption Log Viewer



| Type | Time | Date | ID | Name | Info | File | Line |
|---|---|---|---|---|---|---|---|
| events | 15:24:18 | 11/18/2004 | XX | DCOpen | Entered | dcapi.cpp | 113 |
| info | 15:24:18 | 11/18/2004 | XX | DCOpen | 192.168.0.3 256 / 128 / CBC | dcapi.cpp | 167 |
| events | 15:24:18 | 11/18/2004 | 1 | DCOpen | Exited: true | dcapi.cpp | 181 |

**Figure 7 - PrintCryption Log Viewer**

Users can see the key size, block length, and mode been used for encryption from the Log Viewer program.

## ACRONYMS

| | |
|---|---|
| AESSD | AES Session Daemon |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| ASIC | Application Specific Integrated Circuit |
| CMVP | Cryptographic Module Validation Program |
| CSE | Communications Security Establishment |
| CSP | Critical Security Parameter |
| DKMD | Decryption Key Management Daemon |
| DLE | Downloaded Emulator Card |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FCC | Federal Communication Commission |
| FIPS | Federal Information Processing Standard |
| HMAC | (Keyed-) Hash MAC |
| HTTP | Hypertext Transfer Protocol |
| IP | Internet Protocol |
| KAT | Known Answer Test |
| LED | Light Emitting Diode |
| LPC | Line Printer Control |
| MAC | Message Authentication Code |
| MLS | Multisite Library System |
| NIST | National Institute of Standards and Technology |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| OS | Operating System |
| PC | Personal Computer |
| RAM | Random Access Memory |
| RNG | Random Number Generator |
| RSA | Rivest Shamir and Adleman |
| SHA | Secure Hash Algorithm |
| SKH | Session Key Header |
| SNMP | Simple Network Management Protocol |
| SP | Secure Platform |
| TCP | Transmission Control Protocol |
| VSS | Visual Source Safe |