

### Ensure the highest level of confidence on your network

Lexmark has successfully implemented the CAC authentication solution across all branches of the military

Government mandates for strong user authentication, data security and information assurance have led the Department of Defense to require that the PKI Certificate on the Common Access Card (CAC) must be used by all DoD employees to verify their identity and security classifications. Employees must use their CACs to authenticate access to the network from their computers. But unless your networked multifunction and scanning devices also require CAC authentication, the network and its sensitive information remain vulnerable.

### Secure scanning, data capture and retrieval—without slowing workflow processes

Workflow functions such as scan to email, scan to network folder, document routing, and image capture for document and records management may leave the network open to unauthorized access. To completely secure the network and comply with information assurance policies, Lexmark has enhanced its first to market CAC-enabled multifunction printers (MFPs), ensuring the secure identification of individuals before they introduce data or documents onto the network, or carry out digital sending and retrieval functions.

Digital information capture functions require strong user authentication to protect against unauthorized access and guard critical data. Lexmark enables this robust authentication by preventing the use of network functions at the MFP, until the user's credentials have been authenticated.

The Lexmark solution ensures that only authorized employees may access the network through its MFPs, giving government agencies another option for enhanced network security protection. Users cannot initiate workflow processes at locked MFPs without first inserting a Common Access Card and obtaining authentication. Since the user's identification is associated with all functions initiated while the CAC is in the reader, an audit trail may also be created to track user activity.

Utilization of the user's credentials from the Common Access Card enhances the scan to email workflow by providing a more secure, personalized experience. Email address lookups may be done without the need for a service account. Outgoing email is addressed utilizing the user's account information eliminating anonymous email. S/MIME support is available for enhanced security and privacy\*. CAC credentials may be used to login to an exchange server via SMTP to validate user authorization prior to sending email.



### Solution Summary

Lexmark's solution improves CAC policy compliance by extending CAC laptop and PC authentication protocols to networked multifunction printers. This solution provides strong authentication, email signing/encryption, home directory access and AD group access to device functions.

#### Lexmark Network Multifunction Printers

Integrates print, scan, copy and fax devices. Merges paper and digital workflow to perform office functions efficiently, reliably and cost effectively – providing secure, flexible access to network information.

#### Lexmark Authentication Software

Validates the user PIN and validity of the CAC to obtain the authorization needed to access the network and use other MFP functions.

#### Common Access Card Reader

Reads CAC data to initiate authentication and secures the card while MFP tasks are performed.

\* This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

The Lexmark CAC solution has a rich set of customization capabilities allowing only an authorized user access to specific workflows. Global restrictions may be set such that all users may print jobs, copy and fax normally without CAC authentication, and only require authentication for scanning and other network functions. Users may also be placed into Active Directory (AD) groups allowing function access only to those who are authorized.

User desktops may be set up with the Lexmark Confidential Print feature so that all print jobs are held at the MFP until the user authenticates with their CAC. For improved workflow efficiency this solution may be integrated with Lexmark's Document Solutions Suite and the Lexmark Print Release solution allowing the user to retrieve the print job at the most convenient CAC enabled Lexmark MFP.

### **Integrated architecture blends hardware and software into a secure network access solution**

The Lexmark Common Access Card authentication solution is comprised of three core components:

#### **Lexmark Network Multifunction Printers (MFPs)**

Lexmark monochrome and color MFPs are an onramp for capturing paper-based data and documents electronically, enabling digital sending, information sharing, and workflow processes – efficiently, reliably and cost effectively. Authorized users may walk up to the MFP and perform any function with no special training—the interactive e-Task touch screen interface is designed for easy, efficient, and flexible access to office functions.

#### **Lexmark Authentication Software**

This Lexmark software validates the CAC credentials and PIN to obtain the certificate chain and authorizes access to the network and use of the MFP functions. User preferences, network folders and application permissions are also retrieved and implemented after authorization.

#### **Common Access Card Reader**

The reader is compliant with the NIST standards for CAC and HSPD-12 PIV cards. This device reads the CAC data to initiate the authentication process and secures the card in the device while the MFP tasks are performed.

## Lexmark Responsible Eco-Leadership

### **Responsible Provider of Products and Services**

- EPA's Design for the Environment (DtE) Program
- Packaging Reduction Initiatives
- Product Eco-Labels
- Cartridge Collection Programs
- Product Collection Programs
- Reduce, Reuse, Recycle Campaign

### **Steward of Resources**

- Reduce, Reuse, Recycle Campaign
- Energy Conservation
- Waste Minimization
- Cartridge Remanufacturing and Recycling
- Product Recycling

### **Corporate Citizenship**

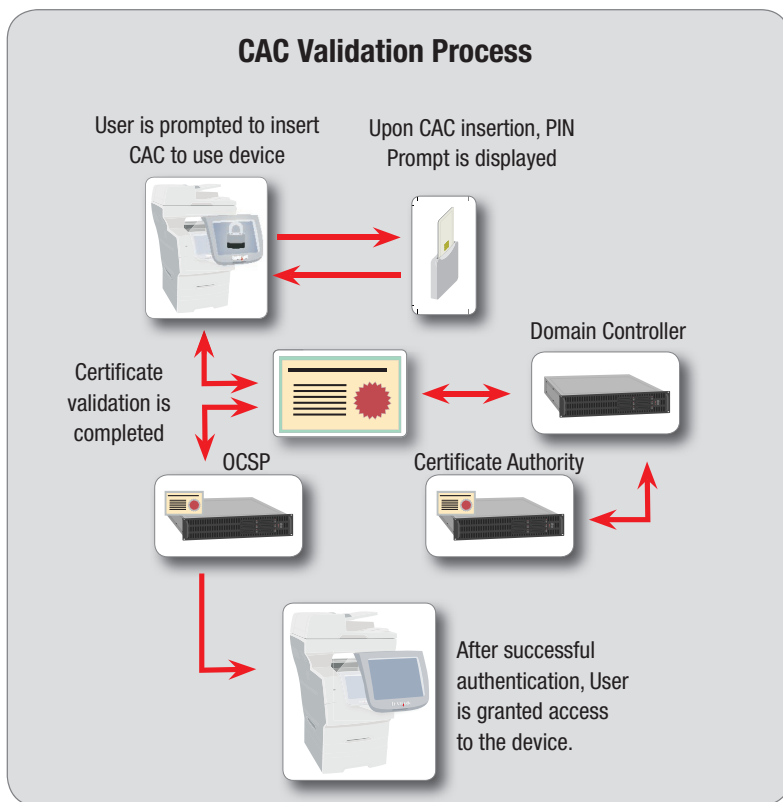
- Environmental Management System
- Consistent Regulatory Compliance
- Cartridge Remanufacturing and Recycling
- Environmental Partnerships with Community



**Authenticate users and keep workflow moving efficiently and securely in four simple steps**

Lexmark’s CAC solution for MFPs follows the same protocol as current laptop and PC CAC authentication processes. The onboard CAC reader and user-friendly e-Task MFP touchscreen make authentication simple and secure:

1. The user inserts their CAC into the MFP’s card reader and is prompted to enter their PIN.
2. The MFP validates the PIN against the CAC, then extracts the PKI certificates from the CAC and sends them to the Windows domain controller for validation. The domain controller response may be validated at the MFP or against an OCSP responder/ repeater.
3. When validation is successful, the MFP home screen appears and user preferences and other system parameters are also implemented. The user can then perform any of the MFP functions such as scan to email (digitally signed and encrypted), scan to home (or other) network folder, scan to document management system, etc.
4. By leaving the CAC in the reader, no additional login is required to perform additional MFP functions. The user will remain logged in as long as their CAC stays in the reader—removing the CAC will return the MFP to its locked, secure state.



**Put Lexmark’s CAC authentication solution to work, keeping your network secure**

By seamlessly integrating Lexmark MFPs and CAC authentication technology, Lexmark can help you meet government security requirements while protecting your network and information from unauthorized access. Utilizing new Lexmark MFPs or adapting your existing fleet, our workflow experts can design and implement a solution that meets your specific departmental requirements.

**Lexmark Global Services**

Lexmark’s Distributed Fleet Management is working for companies around the world.

**Consumables Management**

- Automatic Toner Low Detection
- Automatic Ordering
- Easy, Quick Fulfillment
- Usage Reporting & Color Control

**Availability Services**

- Dedicated On-Site Technicians
- Help Desk Integration
- Advanced Technical Support
- Proactive Maintenance

**Optimization Services**

- Assess the Environment
- Build Deployment Principles
- Apply Business Rules
- Streamline Implementation

**Asset Lifecycle Infrastructure**

- Total Visibility to the Fleet
- Comprehensive Reporting
- Multi-Vendor Support
- Advanced Systems Architecture

## It's Like Getting Increased Infrastructure 'In-A-Box'

### Productivity Right Out of the Box

Fully-integrated Lexmark multifunction printers with a color touch screen allow you to manage documents more effectively. Big, colorful and easy to use, the new e-Task touch screen puts powerful output features to work with just a touch. Customize the touch screen interface with Lexmark's new embedded solutions framework to automate complex business processes.

- **e-Task Interface** – Customizable, vivid and familiar icons on the Lexmark e-Task 8-inch color touch screen provide access to print, copy, fax and scan-to-email functions or custom workflows.
- **Scan Preview** – The ability to view the first page of a scanned document before sending helps ensure accuracy. This is standard on the X646e, X646dte, X850e, X852e, X854e, X782e, X940e and X945e.
- **Job Build** – When scanning jobs that include both the automatic document feeder (ADF) and the flatbed, the entire job can be saved as a single file.
- **Mixed Original Sensing** – When mixed sizes of documents are placed in the ADF, this feature ensures that the appropriate paper size is selected in the copy process.

### Beyond Standard Security

Your business invests in securing networked PCs and servers, so why not secure your printers and MFPs? All high-function network devices should be protected against attack and configured to support your network security policies. Lexmark's MFPs and printers support best industry practices for network device protection. Lexmark devices can be managed securely through an array of industry-standard functions that suit your needs.

- **IPSec** – All network traffic to and from printers and MFPs is encrypted and authenticated.
- **SNMPv3** – Lexmark MFPs support SNMPv3, including authentication and data encryption, to allow secure remote management of the devices.
- **TCP Connection Filtering** – Printers and MFPs can be configured to allow TCP/IP connections from only a specified list of TCP/IP addresses.
- **Operator Panel Lock** – Lock a printer or MFP operator panel, entirely or to administrators only, requiring a PIN number to unlock it.
- **Hard Disk Encryption** – An MFP hard disk can be configured using a 128-bit AES key that encrypts all data on the drive.
- **MFP Lockout** – MFPs can be locked so that the touch screen is disabled and all incoming print and fax jobs are stored securely on the hard drive until the MFP is unlocked by entering the appropriate PIN.
- **Confidential Print** – Hold print jobs until the intended recipient enters an appropriate PIN number that allows the job to be printed.

### Award-Winning Printers



The award-winning Lexmark printers include many features right out of the box. The only limit to what your business can do with these devices might just be your imagination.



CRN - Test Center  
Recommended rating



BERTL - 4 out of 5 stars,  
"Highly Recommended"  
rating



InfoWorld - 8.2 out of 10-  
Very Good rating

### For More Information:

Contact Your Lexmark Representative  
or visit [www.lexmark.com/federalesolutions](http://www.lexmark.com/federalesolutions)

For more information on Lexmark products and services please visit [www.lexmark.com](http://www.lexmark.com)

Lexmark reserves the right to change specifications or other product information without notice. References in this publication to Lexmark products or services do not imply that Lexmark intends to make them available in all countries in which Lexmark operates. LEXMARK PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Buyers should consult other sources of information, including benchmark data, to evaluate the performance of a solution they are considering buying. Lexmark and Lexmark with diamond design are trademarks of Lexmark International, Inc. registered in the United States and/or other countries. All other trademarks are the property of their respective owners. © 2007 Lexmark International, Inc. 740 W. New Circle Rd., Lexington, KY 40550 71K7110