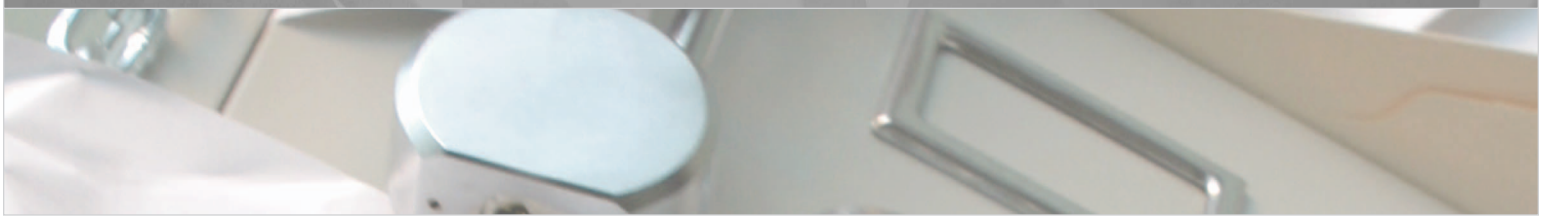

Solution Summary

Lexmark's solution improves CAC policy compliance by extending CAC laptop and PC authentication protocols to networked multifunction printers to provide strong authentication, prevent anonymous scan to e-mail and enable home directory access.

Lexmark Network Multifunction Printers
Integrated print, scan, copy and fax devices merge paper and digital workflow for easy and efficient capture, indexing and flexible access to your company's critical information.

Lexmark Authentication Software
Validates the user PIN and validity of the CAC to obtain the certificate chain needed to authorize access to the network and use of the MFP functions.

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

Close a network security gap and enable information assurance with Lexmark's CAC authentication solution

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) 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 can all leave the network open to unauthorized access. To completely secure the network and comply with information assurance policies, Lexmark has introduced the first CAC-enabled multifunction printers (MFPs), ensuring the secure identification of individuals before they introduce data or documents into 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 after the user's CAC has been authenticated.

The Lexmark solution ensures that only authorized employees can 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 can also be created to track user activity.

The solution can also be set up so that the MFP can print jobs, copy and fax normally without CAC authentication, and only require authentication for scanning and other network functions. User desktops can also be set up with the Lexmark Confidential Print feature so that all print jobs are held at the MFP until the user authenticates printing with their CAC.

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 can 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 and PIN to obtain the certificate chain and authorize access to the network and use of the MFP functions. User preferences, network folders and applications permissions are also retrieved and implemented after authorization.

Common Access Card Reader
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

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 touch screen make authentication simple and secure:

1. The users insert their CAC into the MFP's card reader and are 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 authentication system for validation.

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, scan to home (or other) network folder, scan to document management systems, etc.

4. 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 to keep 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.

Every day, Lexmark color and monochrome multifunction printers go to work for some of the world's most important companies. **And their performance hasn't gone unnoticed.**

Lexmark Multifunction 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.

Centralized Devices

Lexmark X850e
Lexmark X852e
Lexmark X854e

Distributed Devices

Lexmark X644e
Lexmark X646e
Lexmark X646dte
Lexmark X772e

Productivity Right Out of the Box

Easy-to-use, 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 or Lexmark Document Solutions Suite Software to access electronic forms and 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 and X772e.

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.

Priority Copy (Job Interrupt) – For convenience copying, this feature allows you to temporarily interrupt a print job, then resume once the copy is made.

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.

Job Cancel – This intuitive feature clearly lists all jobs in each queue (print,copy, fax) to ensure cancellation of the correct job.

Direct USB Scanning/Printing – Print image files directly from a USB flash drive or scan documents and save them as pdf, tif or jpeg files onto a USB flash drive.

Security Standard

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.

Confidential Print – Hold print jobs until the intended recipient enters an appropriate PIN number that allows the job to be printed.

Operator Panel Lock – Lock a printer or MFP operator panel, entirely or to administrators only, requiring a PIN number to unlock it.

TCP Connection Filtering – Printers and MFPs can be configured to allow TCP/IP connections from only a specified list of TCP/IP addresses.

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.

SNMPv3 – Lexmark MFPs support SNMPv3, including authentication and data encryption, to allow secure remote management of the devices.

IPSec – All network traffic to and from printers and MFPs is encrypted and authenticated.

Secure User Authentication – MFP functions can be restricted so that users must authenticate prior to performing copy, scan-to-e-mail, scan-to-fax, scan-to-network, workflow scripts or embedded applications.

Secure LDAP over SSL – Information exchanged via LDAP, including user credentials, names, e-mail addresses and fax numbers, is encrypted to preserve the confidentiality and privacy of data.

LEXMARK
740 New Circle Rd., Lexington, KY 40550

For more information on Lexmark products and services please visit **www.lexmark.com**

71k7101