

WHITE PAPER

Securing MFPs in a CAC Environment: Today and Tomorrow

Critical Considerations

Contents

The Mandate for Increased Security 1

Key Considerations... 1

Critical Security Level Considerations 1

Platform Flexibility 3

The eCopy CAC Implementation 4

Summary..... 5

Today's sophisticated network copiers or multifunctional products (MFPs), integrate copier, scanner, printer and facsimile functionality into a single platform, with the added capability of network-based document capture, storage and distribution. A primary on-ramp to the government's network, these devices can convert hardcopy documents into easily shared digital files.

As a centralized network document processing hub, MFPs can also pose a potential risk to mission-critical information and applications. Theft or redirection of data is a danger when anonymous walk-up usage is possible. With an expanding MFP installed base deploying safeguards that ensure that only authorized users gain access to the device is not only a best practices imperative, but a federal mandate.

The Mandate for Increased Security

The driving force behind the MFP security initiative is Homeland Security Presidential Directive-12 (HSPD-12). HSPD-12 specifies that all U.S. government employees must use a common identification standard to access physical facilities and information systems that access classified and unclassified networks, as well as network peripherals, such as MFPs. That standard is the Common Access Card (CAC)¹ used within a public key infrastructure (PKI), a system originally developed for the U.S. Department of Defense (DoD).

Based on HSPD-12, office equipment manufacturers and solution providers have moved quickly to develop government-specified two-factor MFP CAC authentication products. Simply called "MFP CAC solutions," these products support CAC cryptographic log-on capabilities for utilization of DoD-certified CAC technology and public key-enabled applications. In short, government-approved MFP CAC solutions must secure the device by requiring walk-up users to be authenticated on the DoD's Certificate Authority server, a far more secure way to lock down the device than entry of a username and password.

Key Considerations

Discretion in design of these solutions has raised concern that many military branches within the DoD source products they think will meet the HSPD-12 mandate.

In fact, they may be leaving their networks wide open, thus vulnerable to a security breach. Indeed, five of the six MFP CAC solutions available today employ an embedded architecture that runs on a proprietary operating system, or web interface, that may not meet the DoD's security standards, potentially putting sensitive information at risk. That said, it is critical to gather detailed information when evaluating MFP CAC solutions. To begin that process, seek answers to the questions related to two key areas, Security Levels and Platform Flexibility.

¹ Federal agencies are migrating to the Federal Information Processing Standard 201 (FIPS 201) Personal Identity Verification (PIV) card. The PIV and CAC have the same form factor, but the PIV provides for interoperability across all federal agencies. Regardless of form, all federal civil servants and members of the military are issued a smart card as a condition of their employment.

Critical Security Level Considerations

Does the MFP CAC solution address security on multiple levels, specifically Device, File, Network, and User levels?

Device Security

Is the user authenticated directly to the domain/Active Directory® list?

After a user is successfully authenticated at the MFP, does the session allow the user Microsoft Active Directory access using LDAP, so the global address book and folder permissions are securely obtained?

Note: This ensures that the solution ties into the existing user management infrastructure.

Does the solution support secure single-session log on for all functions?

In other words, when moving between applications, do you have to log in/out to switch functions, for example, move from Copy mode to Scanner mode?

File Security

Does the solution provide for secure file deletion?

Put another way, when documents are deleted, does the solution comply with the DoD's clearing and sanitizing standards by overwriting the file contents according to DoD 5220.22-M?

Can PDF files be encrypted and password-protected?

In other words, can the file be encrypted and require the recipient to enter a password before the file is viewed, printed, or edited?

Network Security

Does the solution have points of native integration?

More specifically, does the solution work with the native credentialing requirements, e.g., Microsoft® SharePoint®, to provide pass-through authentication to back-end directories?

Does the solution support the Network Drive using secure native file services via SMB?

In other words, does the solution transfer files to, for instance, a back-end file repository through secure channels, thus leverage existing security policies?

Note: Transfer via FTP is not a secure communication method.

User Security

Is user authentication performed using DoD-approved software (middleware)?

More specifically, when the user inserts his/her CAC into the reader, does the CAC solution utilize government-approved Validation Authority (VA) software, such as ActivIdentity and Tumbleweed, to initiate communication with the DoD PKI Server, and, in turn, authenticate the user?

Note: ActivIdentity and Tumbleweed are third-party software solutions that offer a comprehensive, scalable, and reliable framework for real-time validation of digital certificates. Other similar software is available through CoreStreet, VeriSign, or NetSign.

Does the solution support Activity Logging and Document tracking?

In other words, is there an audit trail for each device that records all scan events?

Note: Solutions that supports archival of a backup image, e.g., a PDF, meet federal compliance requirements governing record retention.

Does the solution support Microsoft® Exchange (MAPI) for Scan to Mail, along with digital signature?

Put another way, can the user digitally sign e-mail, whereby the signature is accepted as valid, authentic, and legally binding?

Note: The Army's digital signature policy states that "all e-mails sent from an Army-owned system or account, which contain an embedded hyperlink and/or attachment, must be digitally signed." Not all MFP CAC solutions support digital signature.

Platform Flexibility

Is the MFP CAC solution a prudent investment going forward, that is, built on a platform that can adapt to changing security and compliance requirements?

Is the solution "pre-compliant?"

In other words, does the solution utilize non-proprietary technologies that satisfy DoD security requirements through NIAP, DoD CON, JITC, and Common Criteria, such as ActivIdentity, Tumbleweed, and Microsoft® Windows®?

Note: A solution built on the Windows platform utilizes Microsoft's authentication architecture, which meets the highest validation level of Common Criteria certification — EAL4.

Does the solution facilitate other compliance² mandates?

More specifically, does the solution meet rigorous requirements set forth by HSPD-12, and at the same time, assist with HIPAA and SOX federal mandates.

Note: Any network technology that does not comply with DoD CAC PKI security mandates, including MFPs, may be decommissioned.

Can the solution operate across different MFP or scanner makes/models?

In other words, does the solution offer an open platform, thus operate with legacy products, future models, and mixed fleets?

Note: Embedded MFP CAC solutions are proprietary, thus work with only one make of machine.

Does the solution support more than Scan to Mail?

More specifically, can the solution also authenticate to Scan to File, Scan to Desktop, Scan to Captaris RightFax®, and Scan to Microsoft SharePoint functions?

Note: Some solutions only support limited Scan-to functionality.

² CAC authentication is an identity verification process that not only supports HSPD-12, but also facilitates compliance with federal mandates, such as HIPAA (Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX).

Can the MFP user preview a scan job?

Put another way, can the user see an image of the scanned document on the display before pressing the [Send] button, possibly preventing direction of a file to the wrong recipient?

How are development changes handled?

In other words, if the solution requires a security update, is that process automatic or does the administrator have to push down patches?

Note: Manual implementation of updates, either by batch configuration or direct modification at the device control panel can be time-consuming and inefficient.

Is the solution easy to administer?

More specifically, are software utilities available to minimize IT involvement and streamline management and maintenance?

Does the solution provide a common user interface across the installed base of MFPs?

In other words, does the solution offer a single, consistent user interface that provides IT personnel and users with instant familiarity, regardless of MFP make or model?

The eCopy CAC Implementation

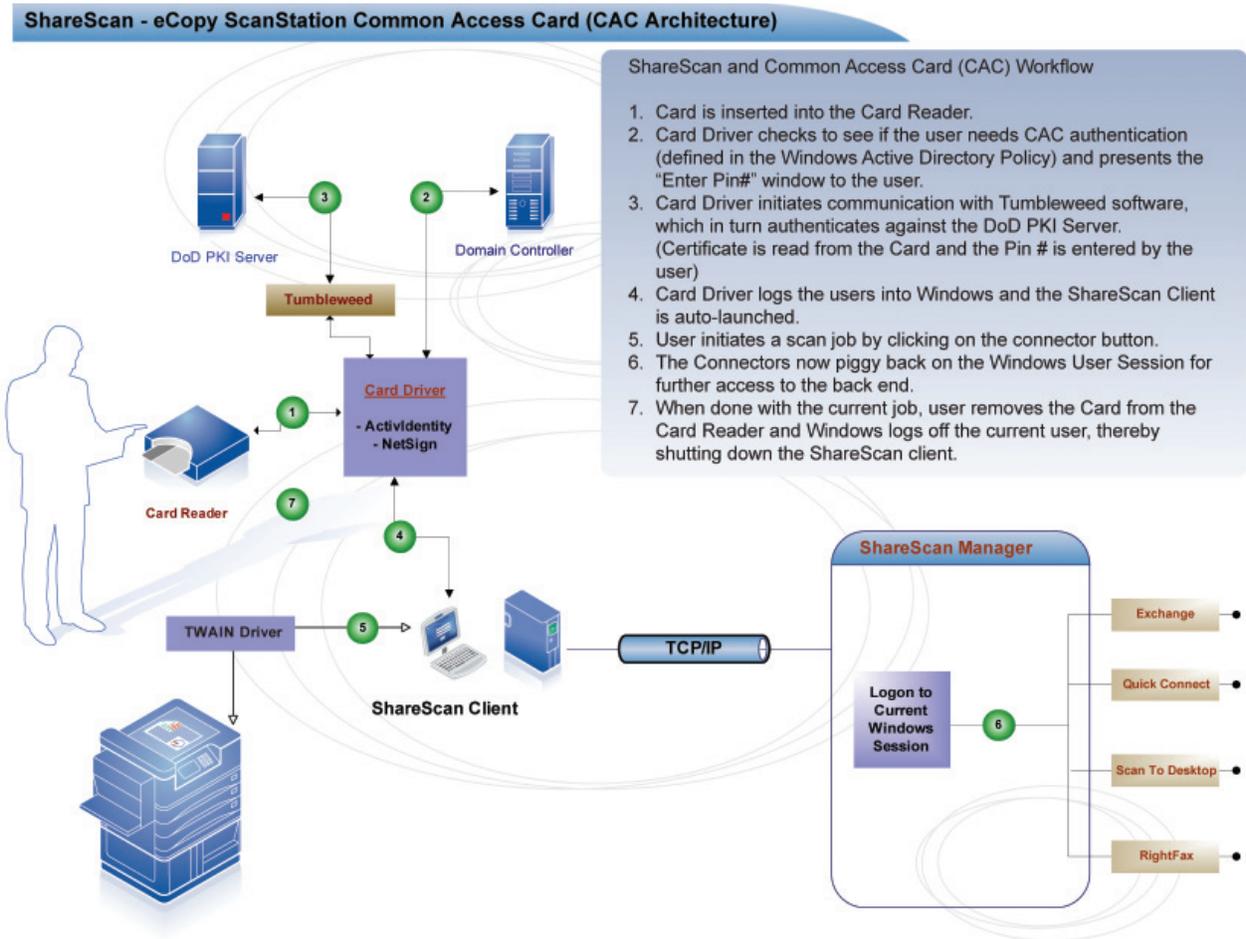
eCopy, Inc., a leading provider of solutions that integrate paper documents into business software applications, offers a “pre-compliant” MFP CAC solution that will enable you to answer Yes to all of the consideration questions.

Unlike other offerings, the CAC-enabled eCopy ScanStation™ (which includes eCopy ShareScan® software)³ runs as a Windows application on the Microsoft operating system, an OS that already adheres to the strictest CAC security requirements, including Common Criteria and others. Furthermore, eCopy’s CAC implementation is “platform-independent,” so users can be authenticated at any compatible MFP equipped with eCopy’s CAC-enabled ScanStation.

The process is simple. The user inserts his/her CAC into the card reader. DoD-approved Validation Authority (VA) software, ActivIdentity or Tumbleweed, automatically communicate with the domain controller and DoD PKI Server respectively, to determine whether or not authentication is required. If so, the user is presented with an “Enter Pin#.”

When the CAC certificate is successfully authenticated, the device unlocks. Removal of the card from the reader shuts the eCopy application down; the user is automatically logged out of the Windows operating system. The MFP’s scanning function is, once again, locked.

³ CAC-enablement services are not available on the eCopy ShareScan embedded platform.



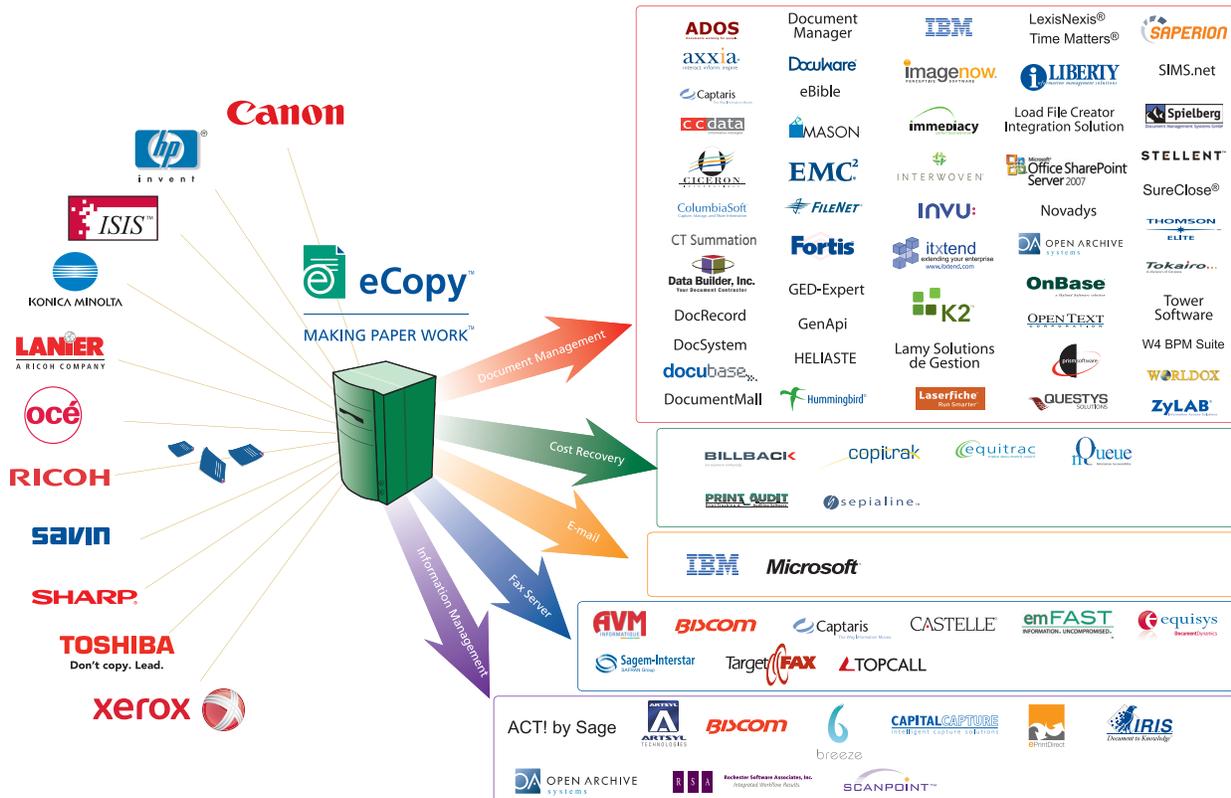
Summary

A highly secure yet flexible solution, eCopy's MFP CAC solution is "pre-compliant" and "platform-independent." These key differentiators mean that the eCopy solution supports interoperability, that is, can be deployed within a mixed fleet of MFP makes and models⁴.

Additionally, when a machine reaches end-of-life, or the lease expires, the CAC-enabled eCopy ScanStation is fully compatible with the new system.

And regardless of MFP make, the system utilizes certified Windows security protocols, maintaining the highest level of security and minimizing risks to every organization's most valuable asset — information.

⁴ eCopy ScanStation is compatible with Canon, HP, Konica Minolta, Lanier, Océ, Ricoh, Savin, Sharp, Toshiba, and Xerox products.



eCopy ShareScan software works with all major MFP brands

Disclaimer

Though no CAC solution can guarantee against all threats to information security, establishing proof of identity at the MFP is a fundamental — and government mandated — starting point.

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.

ONE WAYSIDE ROAD
BURLINGTON, MA 01803

781 565 5000
NUANCE.COM

