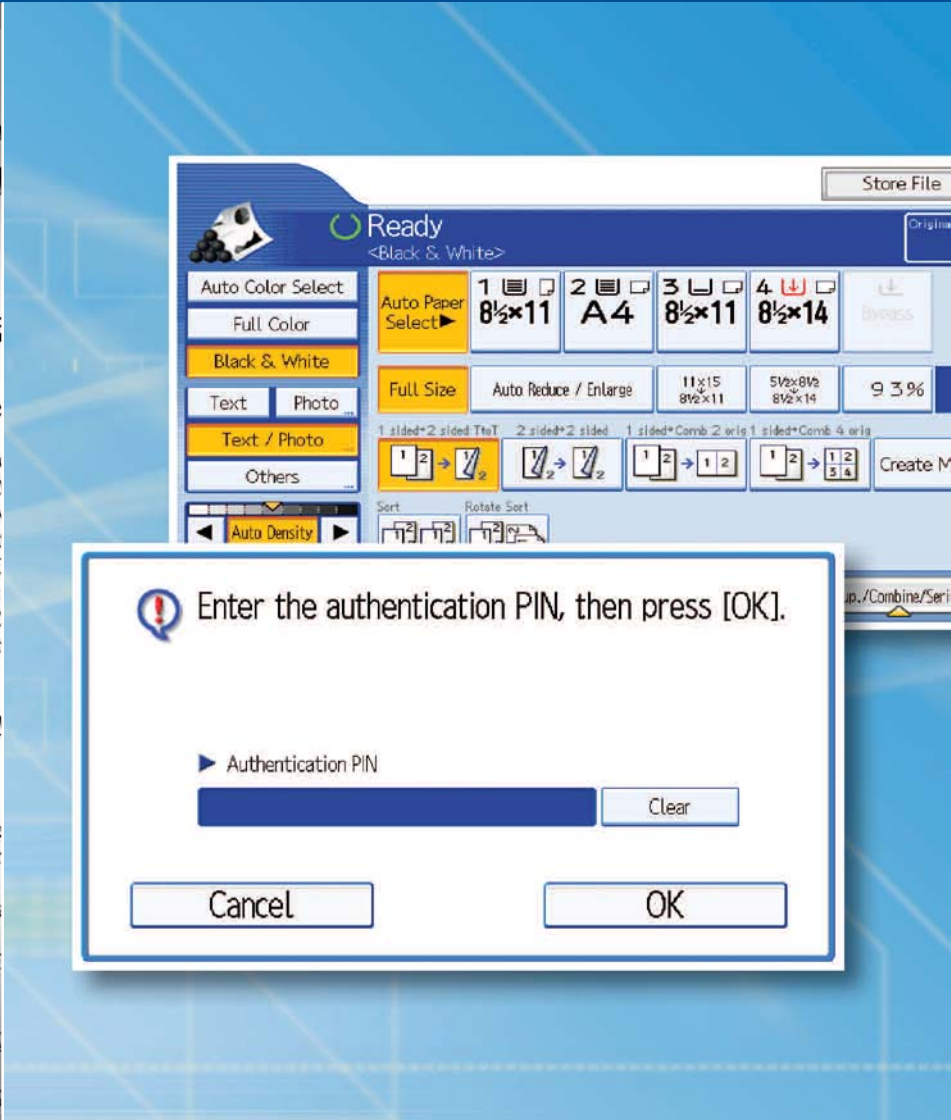




Common Access Card Authentication Solution

SECURE > MONITOR > CONTROL > PROTECT > **SUCCEED >**



Smart Card Technology for the U.S. Department of Defense

Strong User Authentication for Securing Information Assets

The U.S. Department of Defense (DoD) has launched a global initiative to deploy standardized Common Access Cards (CAC), smart cards, to millions of active duty military, reserve personnel, civilian employees and contractors. Among its many functions, the pocket-size CAC allows the card holder to physically access secure areas and permits entry into DoD computer networks. A critical element to this infrastructure is that it requires strong and substantial evidence of the individual's identity.

Information Remains Vulnerable

CAC technology was developed in response to government directives to secure the DoD computer infrastructure, as well as other vital assets, including connected MFPs (multifunctional products). Without access controls in place, MFP users are free to capture, distribute, store and retrieve digital data via the network. As such, digital imaging systems pose a threat to information security.

SAVIN® Addresses Vulnerabilities

Savin developed the CAC Authentication Solution as a tool that allows only holders of a valid CAC to access device functions. Simple yet effective, the Savin solution permits the authenticated user to perform Copier, Scanner, Facsimile and/or Document Server functions.* This strong authentication method allows DoD departments, agencies, officers, employees and contractors to comply with mandates to implement a common identification standard that enhances security and efficiency, while protecting personal privacy.

How it Works

All Savin MFP functions* are locked until the user inserts their valid CAC into the card reader (attached to the device) and enters their Authentication PIN. The user's CAC credentials, embedded on the card, are automatically compared against the DoD's database of authorized users. During the authentication process, the exchange of credentials results in success (identity is confirmed) or failure (identity cannot be confirmed).

Under CAC Authentication, it is also possible to specify which functions can be performed. Device A may allow users to access all functions, while Device B users can only access Copier functions.

www.savin.com

Savin Five Dedrick Place, West Caldwell, NJ 07006
Savin® is a registered trademark of Ricoh Americas Corporation.
All other trademarks are the property of their respective owners.
Specifications and external appearances are subject to change without notice.



Selective authentication controls how data is introduced into a digital workflow; for instance, Scan-to-Email functions can be restricted to only certain areas. This eliminates the anonymous use of Scan-to functions that can lead to potentially damaging information leaks.

*Authentication of Printer functions is handled on the PC level using the DoD's existing desktop policies regarding CAC Authentication.

If the MFP is configured to do so, the authenticated user is automatically registered in the MFP's local address book. This enables the user to easily scan documents to his/her e-mail address, while also preventing anonymous Scan-to-Email. (The CAC must contain the card holder's e-mail address in order for the MFP to register the address.)

Meeting the Urgent Need

Digital imaging systems have become the great enabler for sharing knowledge across an enterprise. However, advances in digital technology have led to unauthorized collection of confidential, classified or proprietary documents and data. To address this growing security challenge, Savin suggests taking a multilayer approach to security, one that includes the Savin CAC Authentication Solution, a tool that effectively safeguards MFP resources, while also supporting government-wide security initiatives.

For more information about the Savin CAC Authentication Solution, contact your Savin sales representative or visit www.savin.com.

SAVIN CAC-COMPATIBLE MFPs

- Savin 8025e/8030e
- Savin 8035e/8045e
- Savin C2525/C3030
- Savin C3535/C4540
- Savin 9025/9033
- Savin 9040/9050
- Savin 8055/8065/8075
- Savin 8060/8070/8080
- Savin C6055/C7570

SAVIN-TESTED SMART CARD READERS

- SCM Microsystems: SCR331 or SCR3310
- OMNIKEY: CardMan 3121

CUSTOMER-SUPPLIED ITEMS NEEDED PRIOR TO INSTALL

- Common Access Card
- Common Access Card Reader
- Common Access Card OCSP Server

REQUIRED DOD SECURITY CERTIFICATES

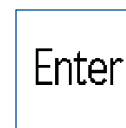
- OCSP Server URL
- OCSP Server Certificate
- Root CA Certificate
- Sub CA Certificate

SPECIFICATIONS

- MFP must be equipped with the Printer/Scanner Kit
- MFP's USB Host Interface is a required option. USB Host Interface is not required for 4.x MFPs.
- MFP's Java VM Card is a required option



1. Insert a valid Common Access Card into the card reader.



2. Enter your Authentication PIN.



3. Identity is confirmed allowing access to secure MFP device functions.