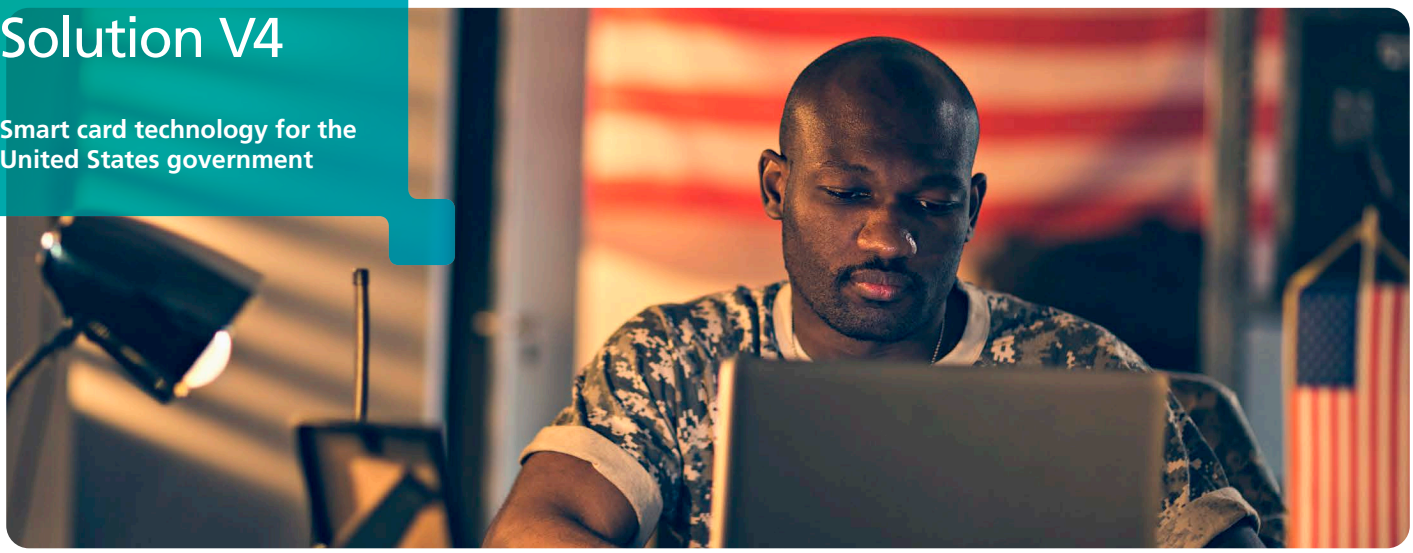
RICOH CAC/PIV Authentication Solution V4

Smart card technology for the United States government

RICOH
imagine. change.



Ensure consistent user authentication

Help ensure customers' information is secured and simplify multifunction printer (MFP) processes with the RICOH Common Access Card (CAC)/ Personal Identity Verification (PIV) Authentication Solution V4, which allows only valid CAC/PIV card holders to access device functions — including scan, copy, scan-to-email, scan-to-folder, fax and document server tasks.* Plus, the user-authentication helps you:

- Protect personal privacy
- Implement a common identification standard across federal government departments and agencies
- Make MFP workflows more efficient for your employees and contractors

Improve document protection and guard against information leaks

Help safeguard information by keeping MFP functions locked until a user inserts a valid CAC/PIV card into your MFP's connected card reader and enters an authentication PIN. During authentication, the user's CAC/PIV card credentials are compared against a database of authorized users. If the user's identity is successfully confirmed, MFP functions become available.

Plus, you can easily manage device activity with selective authentication — choosing which MFP functions can be performed based on user and location. For example, you can:

- Grant access to all functions for Device A users
- Limit access to copy functions for Device B users
- Restrict scan-to-email functions to specific areas

Eliminating the anonymous use of scan-to tasks will help you avoid information leaks.

Meet U.S. government smart card requirements

CAC/PIV smart cards are now required by the federal government for millions of active-duty military personnel, reserve personnel, civilian employees and contractors. These pocket-size cards provide strong and substantial evidence of each individual's identity — a critical element that must be met for card holders to gain physical access to secured areas and entry onto government computer networks.

CAC/PIV technology was developed in response to government directives to help ensure vital assets are secured, including computer infrastructures and connected MFPs. Without these access controls in place, you face information security threats every time you capture, distribute, store and retrieve digital data.

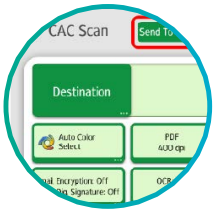
CAC/PIV Authentication Solution

1.

Insert a valid CAC/PIV card into the card reader.

2.

Enter your authentication PIN.



3.

When identity is confirmed, you can access secured MFP functions.

Enhance security when sharing information

Get added protection when capturing and distributing documents over email. Our CAC/PIV Authentication Solution V4 scan-to-email feature allows authenticated users to digitally sign and encrypt emails with Secured/Multipurpose Internet Mail Extension (S/MIME). Only recipients with associated private and public keys can decrypt email messages, helping to ensure document integrity and confidentiality. Plus, users can capture and distribute documents quickly and easily with local MFP and global Lightweight Directory Access Protocol (LDAP) address book search capabilities.

Digitize documents with ease

Transform hardcopy pages into editable PDF files simply with optional Optical Character Recognition (OCR). Quickly search for data by keyword, or import files into a document management system.**

FIPS 140-2 certification for scan-to-email***

Our CAC/PIV Authentication Solution V4 has the encryption and digital signature module validated to Federal Information Processing Standard (FIPS) 140-2 Level1. The FIPS Publication 140-2 is a U.S. government computer security standard issued by the National Institute of Standards and Technology (NIST) — used to accredit cryptographic modules that include both hardware and software components.

Specifications

Supported authentication methods

Common Access Card Authentication Solution supports the following authentication methods:

Online Certificate Status Protocol (OCSP) server
Primary
Secondary
Proxy

Active directory
Kerberos Version 5
Certificate Revocation List (CRL)
Server-based Certificate Validation Protocol (SCVP)

CAC/PIV-compatible Ricoh MFPs

MFP models with SOP G2.0 and higher

Required MFP features

Print/Scan
USB Host Interface

Ricoh-tested CAC/PIV readers

SCM Microsystems: SCR 3310v2
OMNIKEY: CardMan 3121v2

Required customer-supplied items

CAC or PIV cards
OCSP server URL(s)
OCSP server certificate(s)
Root CA certificate(s)
Sub CA certificate(s)

Note: The OCSP Server URL(s) and security certificates must be obtained from the on-site customer security administrator.

For more information, contact your Ricoh sales professional.

* Authentication of printer functions is handled at the PC level using existing desktop policies regarding CAC/PIV authentication.
** MFP must support Optical Character Recognition (OCR) and be equipped with and have the OCR option enabled.
*** Certification pending.

RICOH
imagine. change.

www.ricoh-usa.com

Ricoh USA, Inc., 300 Eagleview Boulevard, Exton, PA 19341, 1-800-63-RICOH

072121

R4152