Canon

Secure, embedded solution for government agencies requiring CAC/PIV authentication to distribute, validate, and secure documents.

Scan-to-E-mail   Scan-to-Fax   Scan-to-Folder

■ **Do you need to comply with directives regarding the use of CAC/PIV technology for network authentication?**

■ **Do you require CAC/PIV authentication prior to sending hard copies to e-mail, network folders, and network fax servers, with an audit trail back to the authorized user?**

■ **Do you require that electronic document communications be encrypted and/or digitally signed?**

To meet the requirements of the Homeland Security Presidential Directive 12 (HSPD-12), the Department of Homeland Security requires Federal agency employees—both civilian and military (DoD)—and their contractors to use standardized Common Access Card (CAC)/Personal Identity Verification (PIV) identification to gain access to facilities and information systems. This standardized identification policy is used to increase security of sensitive information that's contained in, and passes through, information systems. To assist Federal agencies to increase their information security, Canon developed Authorized Send CAC/PIV, a state-of-the art solution that utilizes a powerful two-factor authentication and integrates with your CAC/PIV server to validate credentials before a user can access the document distribution features of their Canon device. This assists in reducing the risk of data being leaked over your network.

Built on the Canon MEAP® architecture, Authorized Send CAC/PIV is an embedded application that's accessible on the touch-screen of the Canon device. It requires no additional server, middleware, or additional end-point protection. Federal employees are required to authenticate using their CAC/PIV prior to sending potentially sensitive information using the scan-to-e-mail, scan-to-fax, and scan-to-folder document distribution features on their Canon MFP devices. Canon further leverages CAC/PIV security by validating a user's CAC/PIV certificate for encryption and digital signatures applied to scan-to-e-mail jobs.

Authorized Send CAC/PIV provides multilayer security out of the box. It's easily configurable, allowing administrators to set parameters, including role-based access to centralized address books (i.e., LDAP or Active Directory). This helps each Federal agency to meet their unique needs for document distribution.

Canon offers Federal agencies an easy-to-use CAC and PIV solution with a large icon-driven, touch-screen interface with support for many card types and card readers, for secure document distribution.

meap

CAC/PIV Authenticated Document Distribution	Secure Scan-to-E-mail/Fax/Folder	CAC/PIV-validated Encryption and Digital Signatures	Serverless Integration	Manage Destinations and Audit Activity	Integrates with Advanced Authentication CAC/PIV
Meets federal two-factor authentication requirement for document distribution. Users must authenticate with their CAC/PIV and enter their PIN code.	Validates CAC/PIV credentials before users distribute scanned documents. Integrates Address Books for quick and accurate scan-to-e-mail and scan-to-fax server.	Allows users to apply a digital signature and up to 256-bit AES encryption that's validated with their CAC/PIV certificate prior to using Authorized Send CAC/PIV to e-mail documents.	Installs directly on Canon device. Requires no additional server or middleware, and supports several protocols including Active Directory, LDAP, and Kerberos.	Enables administrators to restrict document distribution to unauthorized locations (i.e., specific domains, e-mail addresses, or Address Books) and create audit trails.	Allows credential sharing between applications for authorized users to lock down the device and improve efficiency.

User inserts CAC/PIV in reader.

User enters PIN. System authenticates the CAC/PIV user against the compliance server.

After successful authentication, send functions are available for use.

SCAN-TO-E-MAIL

SCAN-TO-FAX

SCAN-TO-FOLDER

SUPPORTED COMMON ACCESS CARD TYPES

Type Name	Applet Type	Platform
End-State PIV Card	PIV End-State + CAC v2	Oberthur ID One v5.2 Dual
End-State PIV Card	PIV End-State + CAC v2	Oberthur ID One 128 v5.5
Transitional PIV Card	PIV Transitional + CAC v2	Gemalto GCX4 72K DI
Emerging Platform	PIV End-State + CAC v2	Gemalto TOP DL GX4 144K
CAC v2	GSC-IS v2.1	Oberthur ID One 128 v5.5
CAC v2	CAC v2	Axalto Access 64K v2
CAC v1	CAC v1	Oberthur CosmopollC v4
CAC v1	CAC v1	Schlumberger Access 32K v2
Axalto ACS 5	Axalto ACS 5	Axalto ACS 5

SUPPORTED CARD READERS

- CCID-Compliant Smart Card Readers
- SCM Microsystems SCR331/3310/3311

SUPPORTED CANON DEVICES

Authorized Send CAC/PIV for imageRUNNER ADVANCE

- imageRUNNER ADVANCE C9075 PRO/C9065 PRO
- imageRUNNER ADVANCE C7065/C7055
- imageRUNNER ADVANCE C5051/C5045/C5035/C5030
- imageRUNNER ADVANCE C2030/C2020
- imageRUNNER ADVANCE 8105/8095/8085
- imageRUNNER ADVANCE 6075/6065/6055

Authorized Send CAC/PIV for imageRUNNER

- Color imageRUNNER C5185/C5185i/C5180/C5180i
- Color imageRUNNER C4580/C4580i/C4080/C4080i
- Color imageRUNNER C3480/C3480i/C3380/C3380i/C3080i/C3080/C2550
- Color imageRUNNER C2880/C2880i
- imageRUNNER 7105/7095/7086*
- imageRUNNER 5075/5065/5055/5050N*
- imageRUNNER 3245/3245i/3235/3235i/3230/3225*
- imageRUNNER 3045/3035/3030/3025*

*The following MEAP-enabled devices are supported in only Windows 2003 PKI environments.

For more information about the Canon Authorized Send CAC/PIV solution, contact your Authorized Canon sales representative or visit www.usa.canon.com.

Canon
*image*ANYWARE

1-800-OK-CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042