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.

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.

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.
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.

### SUPPORTED COMMON ACCESS CARD TYPES

<table>
<thead>
<tr>
<th>Type Name</th>
<th>Applet Type</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-State PIV Card</td>
<td>PIV End-State + CAC v2</td>
<td>Oberthur ID One v5.2 Dual</td>
</tr>
<tr>
<td>End-State PIV Card</td>
<td>PIV End-State + CAC v2</td>
<td>Oberthur ID One 128 v5.5</td>
</tr>
<tr>
<td>Transitional PIV Card</td>
<td>PIV Transitional + CAC v2</td>
<td>Gemalto GCX4 72K DI</td>
</tr>
<tr>
<td>Emerging Platform</td>
<td>PIV End-State + CAC v2</td>
<td>Gemalto TOP DL GX4 144K</td>
</tr>
<tr>
<td>CAC v2</td>
<td>GSC-IS v2.1</td>
<td>Oberthur ID One 128 v5.5</td>
</tr>
<tr>
<td>CAC v2</td>
<td>CAC v2</td>
<td>Axalto Access 64K v2</td>
</tr>
<tr>
<td>CAC v1</td>
<td>CAC v1</td>
<td>Oberthur Cosmopolitan v4</td>
</tr>
<tr>
<td>Axalto ACS 5</td>
<td>Axalto ACS 5</td>
<td>Axalto ACS 5</td>
</tr>
</tbody>
</table>

### 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 C5075 PRO/C9065 PRO
- imageRUNNER ADVANCE C7065/C7055
- imageRUNNER ADVANCE C5051/C5045/C5035/C5030
- imageRUNNER ADVANCE C2030/C2020
- imageRUNNER ADVANCE B105/8095/8085
- 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/C3080i/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.

---

Statements made in this document are the opinions of Canon U.S.A. Canon U.S.A. does not provide legal or regulatory advice concerning customer’s compliance with specific laws including, without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21, the USA Patriot Act, or federal and state privacy laws. Customers should always consult with qualified counsel to determine if they are in compliance with all applicable laws.

CANON, imageRUNNER, and MEAP are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. imageANYWARE is a trademark of Canon. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. All screen images are simulated. Some items may not be available at this time; please check for availability. Specifications and availability subject to change without notice.

©2011 Canon U.S.A., Inc. All rights reserved.

©2011 CACAS-PDF-iH

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

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