


Using the Global Address List (GAL)

PUBLISHING A CERTIFICATE TO THE GAL

1. Insert your CAC into the card reader. Open Outlook. In the **Tools** pull-down menu, select **Trust Center**.
2. In the Trust Center window click the **E-mail Security** tab, and then click the **Publish to GAL** button.
3. Click **OK** to publish your certificates to the Global Address List.

*Note: If your CAC is in the Card Reader you may be prompted to enter your PIN code. Enter your PIN code and click **OK**.*

CHECKING IF A CERTIFICATE'S IN THE GAL

1. Click **New** to compose a **New Mail Message**.
2. Click the **To:** button and choose the recipient from the GAL.
3. Right-click on the recipient's name, and select **Add to Contacts** or **Add to Outlook Contacts**.
4. When the recipient's contact entry appears, click on the **Certificates** icon. 
5. The recipient's certificate should appear in the window. If no certificate is listed, then the recipient's public certificate IS NOT published to the GAL.

BlackBerry and Other Two-way Wireless E-mail Devices (TWED)

E-mails sent from a TWED must be digitally signed if they contain an active (embedded) hyperlink and/or an attachment, or the recipient needs proof of the sender's identity (non-repudiation).

*Reference: Digitally Signing Email BBP, Dated 20 Apr 09:
<https://informationassurance.us.army.mil/bbp/default.htm>*

GOs and SESs are required to have a CAC sled for their BlackBerry devices:

<http://www.tradoc.army.mil/tpubs/misc/cacpki/cappsmemo.pdf>

Required end state is for all BlackBerry users to have CAC readers at some future date:

<http://www.tradoc.army.mil/tpubs/misc/cacpki/sixmonth.pdf>

Receiving a New CAC

When a user receives a new CAC, new PKI certificates are placed on the CAC. These certificates have to be imported onto the user's computer before he can sign outgoing messages or open encrypted incoming messages, and the user needs to upload the E-mail public certificate to the GAL (see the previous page of this Guide). If the user's old certificates are removed from his computer, he will lose the ability to open legacy encrypted messages (those encrypted with the previous CAC). If this happens, the user can recover his old certs from the following website:
<https://ara-1.c3pki.chamb.disa.mil/ara/Key>.

CAC Tools

Three useful CAC/PKI utilities can be found on AKO. Use of these tools has to be coordinated with the user's IMO / DOIM.

1. **CAC Exchange Utility.** The purpose of this tool is to transition legacy encrypted E-mail from one CAC to another while keeping the messages in a secure encrypted state during the transition:
2. **Mailcrypt.** Similar to CAC Exchange Utility.
3. **Card Guard.** The purpose of this tool is to warn users that they have left their CAC in the card reader when they attempt to lock their workstation, log off their system, or shut down their computer.

For Assistance Contact:

- Your ISO/IMO.
- Information Assurance Directorate, Office of the TRADOC DCS, G-6,
monr.tradociapm@us.army.mil.

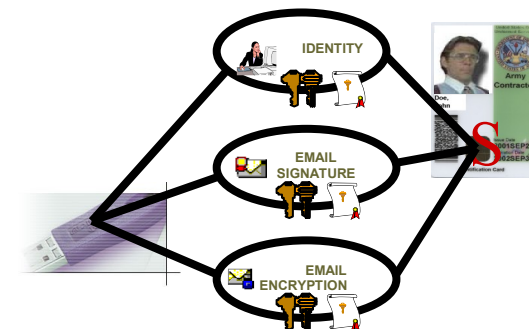
This document is available for download at the following URLs:

<http://www.tradoc.army.mil/tpubs/misc/cacpki/trifold.pdf>
<http://www.tradoc.army.mil/tpubs/misc/cacpki/trifold.pub>

Current as of: 13 May 09



CAC/PKI User's Guide



Overview

COMMON ACCESS CARD (CAC)

The CAC is more than just an ID card. It contains a computer chip, barcodes, and a magnetic stripe which allow it to be used to:

- access buildings and controlled spaces.
- login to computer systems and networks.
- digitally sign and encrypt E-mail messages.

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI is an IT infrastructure that enables users of an unsecured public network (such as the Internet) to securely and privately exchange data. It provides:

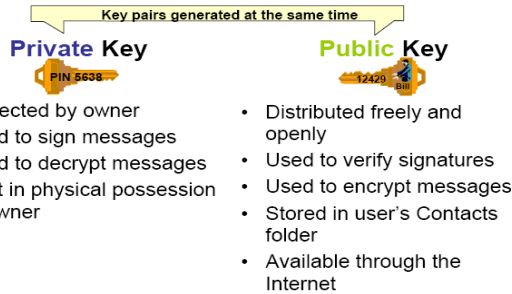
- **confidentiality:** assurance that the person receiving is the intended recipient.
- **integrity:** verification that no unauthorized modification of data has occurred.
- **authentication:** proof that the sender is whom he claims to be.
- **non-repudiation:** assurance that the person sending cannot deny participation.

For more information on CAC or PKI, visit the following website:

http://www.usaarl.army.mil/CBT/EndUser/chapter_01a/chapter01a.html

Certificates and Keys

PKI is a public key cryptography system. In such a system, two keys are generated for each function. One of these keys is kept private, and is hence termed the private key. The other key is widely published and is termed the public key. The diagram below explains the difference between private keys and public keys.



Three DoD PKI certificates, containing public and private keys, are loaded on a CAC. These certificates allow the user to provide digital identification, sign E-mail, and encrypt E-mail.

Rules for Signing and Encrypting E-mail

- **Sending encrypted E-Mail:** E-mail must be encrypted if it contains Personally Identifiable Information or other Sensitive Information (e.g., FOUO).
- **Sending digitally-signed E-mail:** Digital signatures shall be used whenever E-mail contains an active (embedded) hyperlink and/or an attachment, and when the recipient needs proof of the sender's identity (non-repudiation).
- **Do not sign or encrypt E-mail that does not meet the requirements above.**
- **Receiving Encrypted E-Mail:** E-mails that are received in encrypted form must be stored in encrypted form if they are going to be retained.


References:

Digitally Signing Email BBP, Dated 20 Apr 09:
<https://informationassurance.us.army.mil/bbp/default.htm>

HQDA Message, Dated 2 Sep 03:
<http://www.tradoc.army.mil/tpubs/misc/cacpki/message.pdf>


Sending and Receiving Digitally Signed/ Encrypted Messages

SENDING DIGITALLY-SIGNED MESSAGES

1. Insert your CAC into the card reader.
2. Address and compose the message.
3. Before sending, select the Red Ribbon icon.  If this icon is not visible, use the Help feature in Outlook to find how to sign a message, or ask a coworker or your IMO for assistance.
4. Click **Send**. If prompted, enter your PIN and Click **OK**. The Red Ribbon icon appears on the Sent message's envelope.


Note: Messages are signed with the sender's private key. Both PKI and non-PKI recipients can read digitally-signed messages.

SENDING ENCRYPTED MESSAGES

1. Address and compose the message.
2. Before sending, select the Blue Lock icon.  If this icon is not visible, use the Help feature in Outlook to find how to encrypt a message, or ask a coworker or your IMO for assistance.
3. Click **Send**. The Blue Lock icon appears on the Sent message's envelope.

Note: Messages are encrypted with the recipient's public key. Procedures for obtaining public keys are included below.

OPENING ENCRYPTED MESSAGES

1. Encrypted messages have a Blue Lock symbol on their envelope icon.  Only intended recipients with working PKI can open and read encrypted messages.
2. Insert your CAC into the card reader.
3. When you attempt to open an encrypted message, you'll be prompted for your PIN.
4. Enter your PIN and click **OK** to read your message.

For more information on sending or receiving encrypted and/or digitally-signed messages, visit the following website:

http://www.usaarl.army.mil/CBT/EndUser/chapter_01a/chapter01a.html

Storing and Accessing Digital Certificates

In order to encrypt a message, your E-mail software has to have access to a copy of the recipient's public key certificate. There are a number of ways to access certificates.

1. Your E-mail software will automatically find most Army recipients' certificates in the Global Address List (GAL) when you choose to encrypt a message. See the next page of this Guide for more information on using the GAL.

2. The easiest way to obtain a certificate for someone whose E-mail address isn't in the GAL, or who hasn't published his certificate to the GAL, is to import the certificate from a digitally-signed message that the recipient has sent you. For details, visit the following website:

http://www.usaarl.army.mil/CBT/EndUser/chapter_03b_1/chapter03b_1.html

3. You can also download certificates from DoD websites. The two best-known repositories are <http://dodpki.c3pki.chamb.disa.mil> and <http://dodpki.c3pki.den.disa.mil>. There's also a third site, DoD Global Directory Service, <http://iase.disa.mil/gds/index.html>, where users can download certificates; this site may return better search results, and it allows certificates to be saved in different formats.

http://www.usaarl.army.mil/CBT/EndUser/chapter_03b_2/chapter03b_2.html

4. HQDA maintains a file that contains almost all Army General Officer's (GO) and Senior Executive Service (SES) personnel's certificates. This file, and instructions for using it, are at

<https://informationassurance.us.army.mil/cacpki/slcppmain.htm>

5. Store a shared copy of certificates in Public Folders. For users who connect to Microsoft Exchange, creating Contacts folders in the Public Folders hierarchy is a good way to maintain a single copy of certificates that all users on the installation can access.

<http://www.tradoc.army.mil/tpubs/misc/cacpki/folders.pdf>