

Visit the AFPKI SPO Website at:

<https://intelshare.intelink.gov/sites/usaf-pki>

For assistance and additional guidance, contact the AFPKI SPO Help Desk

- Phone: 210-925-2521 (DSN 945)
- Email: [AFPKI.helpdesk@us.af.mil](mailto:AFPKI.helpdesk@us.af.mil)



The AF PKI SPO is part of the Air Force Life Cycle Management Center, C3I & Networks Directorate, Enterprise IT & Cyber Infrastructure Division, Identity Solutions Branch (AFLCMC/HNID), Joint Base San Antonio - Lackland, TX

**DISTRIBUTION C:** Distribution authorized to U.S. Government agencies and their contractors for administrative and operational use.

**HANDLING AND DESTRUCTION NOTICE:** Handle in compliance with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

OPR: AFPKI SPO Outreach  
OE-13-01-114  
June 2020

# FIRST-TIME CAC USER SECURE EMAIL USING OUTLOOK 2016



AIR FORCE  
PUBLIC KEY INFRASTRUCTURE  
SYSTEM PROGRAM OFFICE



Information in this guide is for CAC holders who have received a new CAC for the first time

**Public Key Infrastructure (PKI)** supports DoD's network security and information assurance efforts through the effective use of digital certificates encoded in the microchip of the Common Access Card (CAC).

PKI certificates are necessary to access unclassified networks, applications, websites and portals, to digitally sign forms, and to digitally sign and encrypt unclassified e-mail messages.

When unclassified e-mail messages are digitally signed and encrypted, they are protected with these PKI assurances:

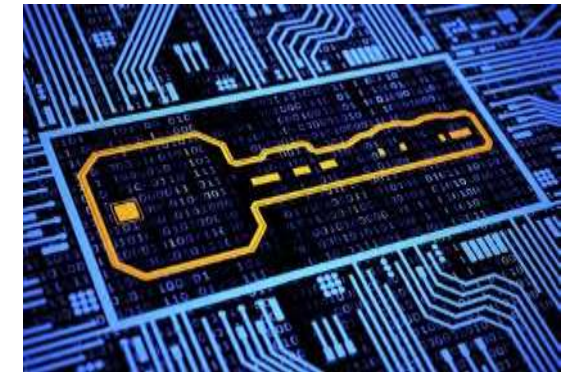
- ✦ **Authentication:** guarantees an e-mail message actually came from the person who claims to have sent it
- ✦ **Data Integrity:** alerts the recipient when unauthorized changes were made to the message during transmission
- ✦ **Non-Repudiation:** legally binds the sender of an e-mail to the transaction
- ✦ **Confidentiality (with encryption only):** assures the information in the e-mail is not disclosed to unauthorized entities



## Why Do You Need This Pamphlet?

A new CAC means new PKI certificates. Follow the instructions in this pamphlet to enable your workstation to successfully recognize and use the PKI certificates on your new CAC.

**This is a User process;  
Administrator privileges are not needed.**



## BUT FIRST,

Insert your new CAC into the card reader. If an error message pops up while trying to use your CAC for the first time, remove the CAC and reinsert it into the card reader.

If the issue persists, reboot the computer (remove the CAC during the reboot process). Once rebooted, reinsert the CAC.

# Never leave your CAC unattended in the card reader

## How to Verify Outlook Security Profile Settings

Upon first use of your newly issued CAC, ensure your Outlook profile is configured properly to digitally sign and encrypt e-mail.

1. Open **Microsoft Outlook**.
  2. Click **File > Options > Trust Center**.
  3. Click on the **Trust Center Settings** button.
  4. At the next window, select **Email Security**.
  5. In the “**Encrypted Email**” area, click the **Settings** button.
    - If all information in the “**Security Settings Name**” window is populated and all boxes are checked, click “**OK**”
- NOTE: “ActivClient Certificates” is an acceptable entry in the “Security Settings Name” field.*
- If information is not populated in the “Security Settings Name” window, type “**My S/MIME Settings (your e-mail address in parenthesis)**”
  - If the **Signing** and **Encryption Certificate** windows are not populated, click “**Choose**” and select the appropriate certificate.
6. Once all windows are populated and all three checkboxes are checked, click “**OK**”

## How to Digitally Sign & Encrypt Unclassified E-mail

Any message that contains an embedded web link or has an attachment must be **digitally signed** per Air Force policy.

Any message that contains sensitive information, such as Controlled Unclassified (CUI), For Official Use Only (FOUO), Privacy Act, Personally Identifiable Information (PII), or information covered by the Health Insurance Portability and Accountability Act (HIPPA) must be **encrypted**.

1. Open **Microsoft Outlook**.
2. Click “**New Email**” to open a new message.
3. Address and compose the e-mail as usual.

*NOTE: for **encrypted** messages, click on the “**TO**” button and select addressees from the Global Address List (GAL); this ensures you have the recipient’s most current Public Key.*

4. Secure the message:
  - To digitally sign the message, click on the “**Sign**” icon on the message toolbar.
  - To encrypt the message, click on the “**Encrypt**” icon on the message toolbar.



- If the message contains **PII** or **HIPPA** information, **also** click on the “**PII**” icon to apply the required warning statement.
  - If the message contains **FOUO** information, **also** click on the “**FOUO**” icon to apply the required warning statement.
5. Click “**Send**”
  6. If prompted, enter your **PIN** and click “**OK**”

## How to Receive Digitally Signed & Encrypted E-Mail Messages

### DIGITALLY SIGNED MESSAGES

The PKI security feature **Authentication** enables you to verify the identity of the sender of a digitally signed e-mail message. To do that:

1. Open the e-mail message.
2. Click on the Red Ribbon icon located at the upper right side of the message.



A **Digital Signature: Valid** window opens to allow you to view the details of the sender’s certificate (this is the sender’s Public Key).

3. Click “**Close**” when finished reviewing.

### ENCRYPTED E-MAIL MESSAGES

Another security feature of PKI is **Confidentiality**. It protects the contents of the e-mail message when in transit and at rest.

When you receive an encrypted e-mail message, you must first decrypt it with your Private Key.

1. Open the e-mail message.
2. Enter your PIN when prompted to access the **Private Key** encoded on your CAC.
3. Read the message as usual.

*NOTE: When you close an encrypted message, it remains encrypted. To reply or forward the message, it must be re-encrypted with the new recipient’s public key.*

## How to Obtain a Recipient’s Public Key

To send an encrypted email, you must have the public key of all recipients. If an intended recipient is not in the GAL, request the recipient(s) to send you a digitally signed email.

1. Open the digitally signed email.
2. Right-click on the sender’s name.
3. Click “Save to Outlook Contacts.”
4. Follow the steps on “How to Digitally Sign & Encrypt Unclassified E-mail,” but select from your Contacts instead of the GAL.

## MANUAL KEY RECOVERY PROCESS

If no encryption keys appear when attempting the Automated Key Recovery process, follow these procedures for manual key recovery.

- Open **Internet Explorer**.
- Enter the following URL into the Web browser:  
<https://intelshare.intelink.gov/sites/usaf-pki-SitePages/Key%20Recovery.aspx>
- Click the + sign next to **Manual Key Recovery Process** and follow the instructions
- Allow 5-7 business days to process the request

Visit the AFPKI SPO Website at:

<https://intelshare.intelink.gov/sites/usaf-pki>

For assistance and additional guidance, contact the AFPKI SPO Help Desk at :

- Phone: 210-925-2521 (DSN 945) or
- Email: [AFPKI.helpdesk@us.af.mil](mailto:AFPKI.helpdesk@us.af.mil)



The AFPKI SPO is part of the Air Force Life Cycle Management Center, C3I & Networks Directorate, Enterprise IT & Cyber Infrastructure Division, Identity Solutions Branch (AFLCMC/HNID), Joint Base San Antonio - Lackland, TX

**DISTRIBUTION C:** Distribution authorized to U.S. Government agencies and their contractors for administrative and operational use

**HANDLING AND DESTRUCTION NOTICE:** Handle in compliance with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

OPR: AFPKI SPO Help Desk  
OE-13-01-114  
June 2020



AIR FORCE  
PUBLIC KEY INFRASTRUCTURE  
SYSTEM PROGRAM OFFICE

# CAC REPLACEMENT SECURE EMAIL USING OUTLOOK 2013-2016



**Information in this guide is for CAC holders who have received a replacement CAC**

**Public Key Infrastructure (PKI)** supports DoD's network security and information assurance efforts through the effective use of digital certificates encoded in the microchip of the Common Access Card (CAC).

PKI certificates are necessary to access unclassified networks, applications, websites and portals, to digitally sign forms, and to digitally sign and encrypt unclassified e-mail messages.

When unclassified e-mail messages are digitally signed and encrypted, they are protected with these PKI assurances:

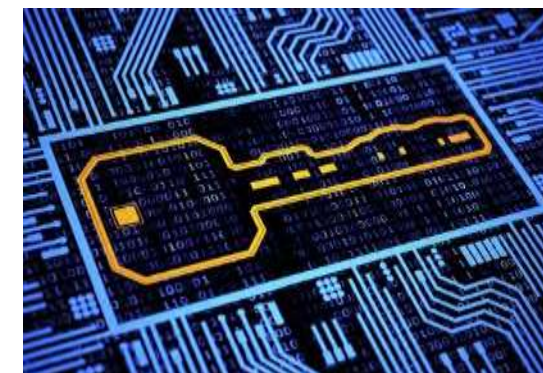
- **Authentication:** guarantees an e-mail message actually came from the person who claims to have sent it
- **Data Integrity:** alerts the recipient when unauthorized changes were made to the message during transmission
- **Non-Repudiation:** legally binds the sender of an e-mail to the transaction
- **Confidentiality (with encryption only):** assures the information in the e-mail is not disclosed to unauthorized entities



## Why Do You Need This Pamphlet?

A new CAC means new PKI certificates. Follow the instructions in this pamphlet to enable your workstation to successfully recognize and use your new PKI certificates.

**This is a User process.  
Administrator privileges are not needed.**



## BUT FIRST,

Insert your new CAC into the card reader. If an error message pops up, remove the CAC and reinsert it into the card reader.

If the issue persists, reboot the computer (*remove the CAC during the reboot process*). Once rebooted, insert the CAC into the reader and proceed to Step 1.

# Never leave your CAC unattended in the card reader

## Step 1: Remove Previous PKI Certificates from IE Certificate Store

- Insert new CAC in the card reader and open **Internet Explorer**.
- Click on the **Tools** icon at the top right-hand corner, then click **Internet Options**.
- Select the **Content** tab > **Certificates** button.
- Select all "old" certificates (CA-31 or higher) with the following exceptions:

### DO NOT SELECT

- Previously recovered e-mail encryption certificates ("CN" in the "Friendly Name" column)
  - "Software" Group certificates used for organizational email accounts
  - ANY DoD email certificates based on expiration dates only
- Click the **Remove** button.

## Step 2: Update Outlook Security Profile Settings

- Remove new CAC from the card reader, then reinsert and open **Microsoft Outlook**.
- Click **File** > **Options** > **Trust Center**, then click the **Trust Center Settings** button (on the right).
- At the next window, select **Email Security**.

- At the next window, in the "Encrypted Email" area, click the **Settings** button.
- In the "Change Security Settings" pop-up, click the **Delete** button until it is grayed out; click **OK**.
- At the "There is no valid security..." pop-up, click **OK**.
- At the "Your Certificates were removed successfully" pop-up, click **OK**.
- Back in the **Trust Center**, click the **Settings** button.
- In the "Change Security Settings" pop-up, click the **Choose** button for **Signing Certificate** and select the most current **DoD Email CA-XX** certificate; if none are showing, click "More Choices" and select the correct certificate; click **OK**.
- In the "Change Security Settings" pop-up, click the **Choose** button for the **Encryption Certificate** and select the most current **DoD Email CA-XX** certificate; click **OK** > **OK**.
- At the warning pop-up, click **OK**; enter your **PIN** if prompted.
- At the "Your certificates were published successfully" pop-up, click **OK**, then click **OK** to exit the **Trust Center** (you may need to restart Outlook).

## Step 3: Recover a Previous Email Encryption Key

Your new CAC contains a new Email Encryption certificate and corresponding encryption key. Any email encrypted with your previous encryption key cannot be opened with the new key; therefore, to read those email messages, you must recover the previous encryption key.

There are two methods to recover an encryption key: **AUTOMATED** (recommended) and **MANUAL**.

### AUTOMATED KEY RECOVERY

- Open **Internet Explorer**.
- Enter one of the following URLs into the Web browser (case sensitive):
  - <https://ara-5.csd.disa.mil/ara/>
  - <https://ara-6.csd.disa.mil/ara/>
- At the "Window Security" pop-up, select an **Identity Certificate**; click **OK**.
- Enter your **PIN** if/when prompted.
- At the "Automatic Key Recovery Agent" page, click **I Accept**; a list of encryption keys will appear.
- Based on the **date range**, select the desired key from the list (**NOTE: the list is not in any order**).
- Click the blue **Recover** button.
- Click **I Acknowledge**, then click **OK**.

- The next screen provides a **Download** link and a **16-character, case-sensitive password**; write the password down **EXACTLY** as shown.
- Click on the **Download** link, then click **Open**.
- Click **Next** at the "Welcome to the Certificate Import Wizard" screen (do not change default buttons).
- Click **Next** at the "File to Import" prompt
- At the "Private Key Protection" screen, click the **Display Password** checkbox, then enter the **16-character password**.
- Verify the password is correct, then click **Next**.
- At the "Certificate Store" prompt, select **Automatically select the certificate store**, then click **Next**.
- At the "Completing the Certificate Import Wizard" screen, click **Finish**.
- At the "Import was successful" pop-up, click **OK**.
- Click **Return to Key List** and repeat these steps to recover other Encryption Keys as needed.

The recovered key(s) is/are now installed in the certificate store and ready for use. When opening previously encrypted email, MS Outlook automatically selects the corresponding encryption key from the certificate store.

