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

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

Air Force
Public Key Infrastructure
System Program Office

First-Time CAC User

Secure Email Using Outlook 2016

Delivering Cyber Defense and Information Assurance Solutions to the Air Force
PKI

Information in this guide is for CAC holders who have received an 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.

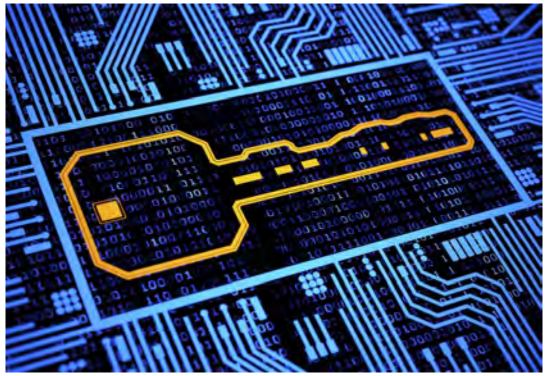
When unclassified e-mail messages are digitally signed and encrypted, they are protected with these PKI assurances:

- 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

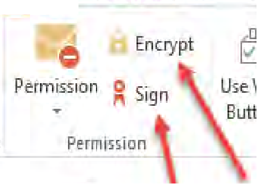
Any message that contains an embedded web link of has an attachment must be digitally signed per Air Force policy.

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.



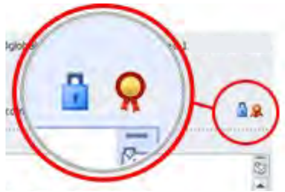
   - If the message contains PII or HIPPA information, *also* click on the **"PII"** icon to apply the required warning statement.
   - If the message contains FOUO information, *also* click on the **"FOUO"** icon to apply the required warning statement.
5. Click **"Send"**
6. If prompted, enter your PIN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