AIR FORCE PUBLIC KEY INFRASTRUCTURE SYSTEM PROGRAM OFFICE

FIRST-TIME CAC USER

SECURE EMAIL USING OUTLOOK 2016

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 your Common Access Card (CAC).

PKI certificates are used to access all DoD unclassified networks, websites, applications, and portals, to digitally sign forms, and to digitally sign and encrypt unclassified email messages.

Unclassified email messages that are digitally signed and encrypted are protected with these PKI assurances:

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

WHY IS THIS DOCUMENT IMPORTANT TO YOU?

At this time, your workstation must be manually configured to successfully recognize and use the PKI certificates on your CAC. Follow the instructions on the next page to ensure proper functionality.

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 log into the network with your CAC for the first time, remove the CAC and reinsert it into the card reader. If the issue persists, remove your CAC and reboot the computer. Once rebooted, reinsert the CAC. If you are still unable to login, contact your local Computer Support Personnel and/or Information Assurance Officer to verify your network account is created and enabled for use.*

The AFPKI SPO is part of the Identity Solutions Branch (AFLCMC/HNID), Joint Base San Antonio - Lackland, TX, organizationally aligned under the Air Force Life Cycle Management Center, Enterprise IT & Cyber Infrastructure Division, EIT & Cloud Capabilities Division.

DELIVERING CYBER DEFENSE AND IDENTITY ASSURANCE SOLUTIONS TO THE AIR FORCE

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

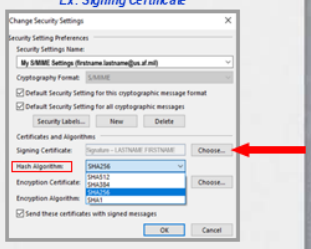
U.S. AIR FORCE

Verify Your Outlook Security Profile Settings

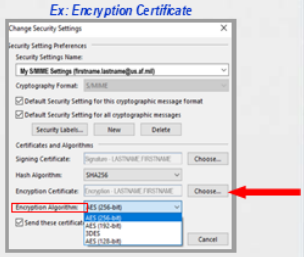
To ensure your Outlook profile is configured to digitally sign & encrypt unclassified email:

1. Open **Microsoft Outlook**, then click **File** > **Options** > **Trust Center** > **Trust Center Settings**
2. At the next window, select **Email Security**
3. In the **"Encrypted Email"** area, click **Settings**
   - If information in the **"Security Settings Name"** window is populated and all boxes are checked, click **"OK"**
   - If information is not populated, type **"My S/MIME Settings (*your email address*)"**
   - If the **Signing Certificate** window is not populated, click the "**Choose**" button and select the **"Signature"** certificate
     - Click the drop-down arrow in the **Hash Algorithm** window and select "**SHA256**"
   - If the **Encryption Certificate** window is not populated, click the **"Choose"** button and select the **"Encryption"** certificate
     - Click the drop-down arrow in the **Encryption Algorithm** window and select "**AES (256-bit)**"
4. Once all windows are populated and all three checkboxes are checked, click **"OK."** Your work-station is now configured to use the PKI certificates on your CAC.

Ex: Signing Certificate



Ex: Encryption Certificate



When & How to Digitally Sign & Encrypt Unclassified Email

Per Air Force policy, unclassified email messages must be **digitally signed** if they contain an embedded web link and/or include an attachment. Messages must be **encrypted** to recipients **outside the Department of the Air Force (DAF) Network** *(i.e., @us.af.mil or @spaceforce.mil)* when they contain sensitive information, such as Privacy Act (PA), Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and information covered by the Health Insurance Portability and Accountability Act (HIPPA).

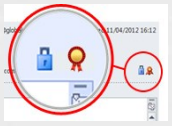
1. Open **Microsoft Outlook**; click **"New Email"** then address and compose the email as usual *(**Note**: for **encrypted** messages, click the **"To"** button and select recipients from the Global Address List (GAL); this ensures you have the recipient's most current **Public Key**, which is necessary to encrypt an email).*
2. Secure the message:
   - To digitally sign the message, click the **"Sign"** icon on the message toolbar
   - To encrypt the message, click the **"Encrypt"** icon

3. Compose email as intended, then click **"Send."** If prompted, enter your **PIN** and click **"OK"**

How to Receive Digitally Signed & Encrypted Email Messages

Digitally Signed Messages: The PKI feature **Authentication** enables you to verify the identity of the Sender of a digitally signed email message.

- Open the email message and click on the Red Ribbon icon located at the upper right side of the message; a **Digital Signature: Valid** window opens with the details of the sender's certificate *(this is the sender's **Public Key**)*; click **"Close"** when finished.



Encrypted Email Messages: Another PKI feature is **Confidentiality**, which protects the contents of the message while in transit. Encrypted messages must first be decrypted with your **Private Key**.

- Open the email message, and if prompted, enter your PIN to access your **Private Key** encoded on your CAC

***NOTE**: To reply to or forward an encrypted message, you must re-encrypt the message with the recipients' public key.*

How to Obtain a Recipient's Public Key When Not in the GAL

To send a encrypted email, you must have the public keys of all recipients, which are easily obtained from the GAL. However, if any intended recipient is not in the GAL, simply request a digitally signed email message from the recipient(s) and save their Public Key.

1. Open the digitally signed email and right-click on the sender's name
2. Click **"Save to Outlook Contacts"**
3. Follow the steps above but select the recipients from your **Contacts List** instead of the GAL

For More Information...

For more PKI related information, visit the AFPKI Website at https://go.intelink.gov/AFPKI *(case sensitive; CAC required)*

For PKI technical support, contact the AFPKI Help Desk at 210-925-2521 (DSN 945) or E-mail: afpki.helpdesk@us.af.mil