# AF PKI SPO

## First-Time CAC User
## *Secure Email Using Microsoft Outlook*

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

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

## Why is this Document Important to You?

At this time, your NIPRNet 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 onto 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 still unable to log in, contact your local Computer Support Personnel and/or Information Assurance Officer to verify your network account has been created and enabled for use.* Do not return your CAC to the CAC issuance facility.

**Digitally signed & encrypted** email messages and documents are protected with these PKI assurances:

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

*Digital Signatures facilitate a trusted exchange of communications.*
*They are intended to solve the problem of tampering and impersonation.*

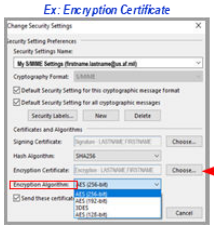
## Verify Your Outlook Security Profile Settings

The first step is to ensure your Outlook profile is configured to digitally sign & encrypt unclassified email:

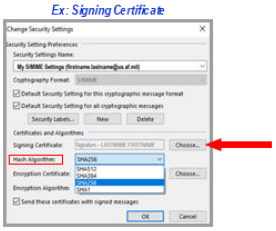
1. Open **Microsoft Outlook**, then click **File** > **Options** > **Trust Center** > **Trust Center Settings**
2. At the next window, select **Email Security**
3. In the **Encrypted Email** area, click the **Settings** button
   - 🗝 If information in the **Security Settings Name** window is populated and all boxes are checked, click **OK**
   - 🗝 If information is not populated, type **My S/MIME Settings (*your email address*)**
4. 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)**, click **OK**
5. 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**, click **OK**
6. Once all windows are populated and all three checkboxes are checked, click **OK**

Your workstation is now configured to use the PKI certificates on your new CAC.

*Ex: Encryption Certificate*



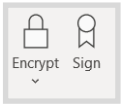
*Ex: Signing Certificate*



## When & How to Digitally Sign & Encrypt Unclassified Email

Per Air Force policy, unclassified email messages must be **digitally signed** when they contain an embedded web link and/or include an attachment. Messages must be **encrypted** to recipients **outside the .MIL and NSA.GOV networks** *(e.g., @us.af.mil, @spaceforce.mil, @army.mil, @nsa.gov)* 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). Per GENADMIN 2024-1118, *CUI/PII/PHI Security Update,"* email that remains withing .MIL and NSA.GOV domains are sufficiently protected and do not require additional encryption.

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) to get the recipient's most current Public Key, which is necessary to encrypt an email)*
2. Compose email as intended
3. To secure the message, click on **Options** at the top of the new email
   - To digitally sign the message, click the **Sign** icon on the message toolbar
   - To encrypt the message, click the **Encrypt** icon on the message toolbar
4. Click **Send**; enter your **PIN**, if prompted, 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 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)*

**Encrypted Email Messages**: Another PKI feature is **Confidentiality**; it protects the contents of the message while in transit. To read an encrypted message, it 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**: When replying to or forwarding an encrypted message, you must re-encrypt the message with the public keys of all recipients.*

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

To send an 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 and **Save** their Public Key to your **Outlook Contacts**.

- Open the digitally signed email, right-click on the Sender's name, then click **Save to Outlook Contacts**
- Follow the steps above but select the recipients from your **Contacts List** instead of the GAL

***For more PKI-related information, visit the AF PKI SPO Web Site at:***
https://go.intelink.gov/AFPKI *(CAC required)*

***For PKI technical support, contact the AF PKI Help Desk at:***
https://afpki.servicenowservices.com

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