AF PKI SPO

CAC Replacement Guide

Secure Email Using Microsoft Outlook

Congratulations! You've just been issued the new, modernized Common Access Card (CAC).

The new, modernized CAC contains common identity standards that enable the US Warfighter's ability to interoperate with various mission partners and reduce inefficiencies around secure information exchange on the NIPRNet.

Externally, your new CAC is similar to your previous CAC. Internally, the modernized CAC contains four single-use certificates, one for each major PKI function. Beyond selecting the PIV-Auth certificate during network logon *(vs. the email certificate)*, your experience with the CAC will not change.

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 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 still unable to log in, contact your local Computer Support Personnel; **do not return your CAC to the CAC Issuance Facility**.

In most cases, the modernized CAC contains the following certificates:

- **Authentication (PIV)**: used to gain logical access to DoD unclassified networks, websites, systems, and applications
- **Signature**: used to digitally sign documents, forms, and unclassified email messages
- **Encryption**: used to encrypt/decrypt unclassified email messages
- **Card Authentication Key (CAK)**: used to gain physical access to US Govt controlled facilities/spaces enabled with Physical Access Control Systems

The AF PKI SPO is aware of the inconvenience of having to complete this 3-step process. With your experience in mind, we've automated the process as much as technologically possible. Our efforts continue toward making CAC replacement a seamless transition.

STEP 1: REMOVE PREVIOUS PKI CERTIFICATES FROM THE CERTIFICATE STORE

a. Insert your new CAC in the card reader and click the **Start** button *(i.e., the Windows icon at bottom left of system tray);* select **Search**

b. In the **Type here to search** box, type **Control Panel**, then click **Open** > **Network and Internet** > **Internet Options**

c. Select the **Content** tab > **Certificates** button

d. Select all "old" certificates **EXCEPT** previously recovered email encryption certificates *(identifiable by **CN=** in the **Friendly Name**)*

e. Click the **Remove** button, then click **OK** at the warning

STEP 2: UPDATE YOUR OUTLOOK SECURITY PROFILE SETTINGS

a. Remove your new CAC from the card reader and reinsert it

b. Open **Microsoft Outlook**, then click **File** > **Options** > **Trust Center** > **Trust Center Settings**

c. At the next window, select **Email Security**

d. At the next window, in the **Encrypted Email** area, click the **Settings** button

e. In the **Change Security Settings** pop-up, click the **Delete** button until it is grayed out; click **OK**

f. Back in the Trust Center, click the **Settings** button

g. In the **Change Security Settings** pop-up, click the **Choose** button for **Encryption Certificate** and select the most current **DoD Email CA-XX certificate**; then click **OK**

   - Verify the **Encryption Algorithm** shown is **AES (256-bit)**; if not, click the drop-down arrow, select **AES 256-bit**, then click **OK**

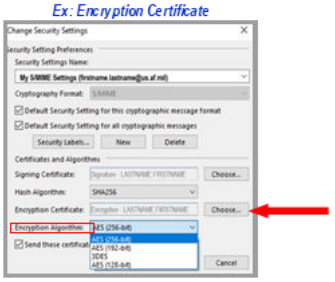
h. Still in the **Change Security Settings** pop-up, click the **Choose** button for **Signing Certificate** and select the most current **DoD Email CA-XX certificate**; if none are showing, click **More Choices** and select the correct certificate, then click **OK**

   - Verify the **Hash Algorithm** shown is **SHA256**; if not, click the drop-down arrow and select **SHA256**

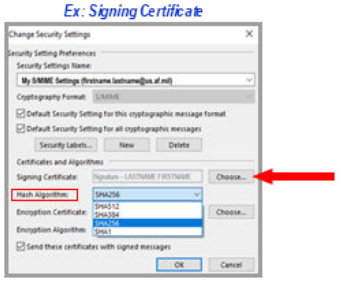
i. At the Warning pop-up, click **OK**; enter your **PIN** if prompted

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



STEP 3: RECOVER A PREVIOUS EMAIL ENCRYPTION KEY

Your new CAC contains a new **Email Encryption Certificate** with a corresponding public/private encryption key pair. Any unclassified email encrypted with your previous encryption key cannot be opened *(i.e., decrypted)* with the new key. Therefore, to continue to read those email messages, you must **recover the previous encryption key**. Fortunately, NIPRNet encryption keys are escrowed for recovery purposes. There are two methods to recover a NIPRNet encryption key: **AUTOMATED** *(recommended)* and **MANUAL**.

AUTOMATED KEY RECOVERY *(NIPRNet)*

a. Open an Internet browser and type in one of the following URLs:

   - **https://ara-5.csd.disa.mil**
   - **https://ara-6.csd.disa.mil**

b. When prompted to choose a certificate, select the **PIV Identity Certificate**; enter your **PIN**, if prompted

c. Read the US Department of Defense Warning Statement, then click the **I Accept** button

d. The **Automated Key Recovery Agent (KRA)** opens with a list of all your escrowed encryption keys available for recovery. **Review** the list to find the serial number and validity dates that match the timeframe of the encryption key you wish to recover *(e.g., validity dates of previous CAC)*.

   - ***NOTE**: "Key Usage" must be **Key Encipherment**; no other certificates can be recovered*
   - ***NOTE**: DO NOT RECOVER any encryption keys with a "Not Valid Before…" date within one day of your newly issued CAC*

e. Click the blue **Recover** button next to the desired certificate

STEP 3: CONTINUED

f. At the pop-up window asking for acknowledgement that you are the subscriber of the selected escrowed key, click **I Acknowledge**, then click **OK**

g. The Auto KRA returns with a **DOWNLOAD** link and a **complex one-time password** *(case sensitive)*

This page is only available for a few minutes, so quickly **write down the password exactly as shown,** or capture a screenshot *(Copy/Paste will not work)*

h. Once you've captured the password, click the **DOWNLOAD** link, then click **Open**

- ***NOTE**: if using **Google Chrome** as your browser, you will be prompted to **Save** the .p12 file to your computer prior to opening it; be sure to **delete** the file after successfully recovering the certificate and **empty** the Recycle Bin*

i. Go to the location of the **saved .p12** file; double-click the file

j. At the **Welcome to the Certificate Import Wizard** window, ensure the **Store Location** radio button is on **Current User**; click **Next**

k. At the **File to Import** prompt, click **Next**

l. At the **Private Key Protection** screen, enter the **16-character complex password** exactly as it was presented to you

- Check the **Display password** box and verify the password is correct, then click **Next**

m. At the **Certificate Store** prompt, click the radio button for **Automatically select the certificate store…**, then click **Next**

n. At the **Completing the Certificate Import Wizard** screen, click **Finish**

o. At the **Import was successful** pop-up, click **OK**

The recovered key is now installed in the certificate store on your computer and ready for use. Microsoft Outlook will automatically find and use this key when opening *(i.e., decrypting)* any email encrypted with the recovered key.

MANUAL KEY RECOVERY *(NIPRNet)*

When attempting the Automated Key Recovery process, if no encryption keys appear, follow these procedures for the **Manual Key Recovery** process.

a. Open an Internet browser and enter *(or copy/paste)* the following URL into the web browser:

https://intelshare.intelink.gov/sites/usaf-pki/SitePages/Manual%20Key%20Recovery%20Process.aspx

b. Download and complete the **Key Recovery Request form**; **save** the completed form on your desktop

c. Submit the completed form to the Air Force Key Recovery Agent (AF KRA) at https://afpki.servicenowservices.com/sp

- Click on **Request Something**
- Click on **Key Recovery Incident**
- Complete the required information, then click **Add attachments** *(paperclip icon)* to **upload** the **Key Recovery Request Form**
- Click **Submit**
- Verify the Key Recovery Request Form is attached
- Enter applicable message; click **Post**

d. Allow 5-7 business days to process the request; if this is urgent, include **URGENT** in the message and provide justification for the urgency

***NOTE**: Encryption keys for classified email are not escrowed. If you also need to recovery SIPRNet encryption keys, go to the SIPRNet AF PKI CoP to obtain a Key Recovery Request form and instructions to submit.*

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 Protect Branch (AFLCMC/HNID), Joint Base San Antonio-Lackland, TX, aligned under the Air Force Life Cycle Management Center, Command, Control, Communications, Intelligence & Networks (C3I&N) Directorate (HN), Enterprise IT & Cyber Infrastructure Division (HNI)