

AIR FORCE PUBLIC KEY INFRASTRUCTURE SYSTEM PROGRAM OFFICE

CAC REPLACEMENT GUIDE

SECURE EMAIL USING OUTLOOK 2013-2016

Congratulations! You've just been issued the new, <u>modernized</u> 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.

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

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

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 steps 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 logging into the network with your new CAC 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; do not return your CAC to the CAC Issuance Facility.



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.



NOTE

The AFPKI SPO is aware of the inconvenience imposed upon you to complete the 3-step process outlined here. With your experience in mind, we have automated the process as much as we can and will continue to work to make the CAC replacement transition seamless.

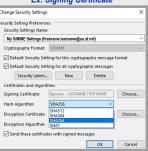
STEP 1: REMOVE PREVIOUS PKI CERTS FROM THE CERTIFICATE STORE

- a. Insert your new CAC in the card reader and click the **Start** button (Windows icon at bottom left of system tray)
- b. Click on Control Panel > Internet Options
- c. Select the Content tab > Certificates button
- d. Select all "old" certificates EXCEPT:
 - ₽ Previously recovered email encryption certificates ("CN=" in the "Friendly Name")
 - ANY DoD email certificates based on expiration dates only
- e. Click the Remove button, then click OK at the warning

STEP 2: UPDATE 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 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
- h. Verify the **Hash Algorithm** shown is "SHA256;" if not, click the drop-down arrow, select "SHA256"
- In the "Change Security Settings" pop-up, click the <u>C</u>hoose button for Encryption Certificate and select the most current DoD Email CA-XX certificate; click OK
- j. Verify the Encryption Algorithm shown is "AES (256-bit);" if not, click the drop-down arrow, select "AES (256-bit)" then click OK
- k. 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: Signing Certificate



Ex: Encryption Certificate

Ex. Eneryption ocitineate			
Change Security Settings			×
Security Setting Preference Security Settings Name:			
My S/MIME Settings (fire	tname.lastname@us.	af.mil)	~
Cryptography Format:	S/MIME	~	
☑ Default Security Setting for this cryptographic message format			
☑ Default Security Setting for all cryptographic messages			
Security Labels	New	Delete	
Certificates and Algorithms			
Signing Certificate:	Signature - LASTNAME	Choose	
Hash Algorithm:	SHA256	~	
Encryption Certificate:	Encryption - LASTNAMI	FIRSTNAME	Choose
Encryption Algorithm:	AES (256-bit)	~	- 1
Send these certificat	AES (256-bit) AES (192-bit) 3DES		
	AES (128-bit)		Cancel

STEP 3: RECOVER A PREVIOUS EMAIL ENCRYPTION KEY

Your new CAC contains a new Email Encryption certificate and corresponding public/private encryption key pair. 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

- a. Open a browser and type in one of the following URLs (case sensitive)
 - https://ara-5.csd.disa.mil/ara/
 - Https://ara-6.csd.disa.mil/ara/
- b. When prompted to choose a certificate, select your PIV-Auth certificate, then enter your PIN if prompted
- c. At the "Automatic Key Recovery Agent" (AKRA) page, click I Accept. Note the list of all your escrowed encryption keys available for recovery. Review the list, then based on the date range, select the key that matches the timeframe of the encryption key you wish to recover.

 Automatic Key Recovery Agent

NOTE: Key Usage must be **"Key Encipherment;"** no other certificates can

NOTE: DO NOT RECOVER any encryption keys with a "Not Valid Before..." date within one day of your newly issued CAC

d. Click the blue Recover button



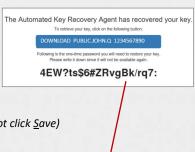
STEP 3: CONTINUED

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



The AKRA returns with a "Download" link and a complex, 16-character, case-sensitive password.

<u>DO NOT</u> click the Download link until you've **written down** the password <u>EXACTLY</u> as shown or captured a screenshot (copy/paste will not work). <u>NOTE</u>: this page is only available for a few minutes.



Type the password for the private key

.....

- f. Once you've captured the password, click on the **"Download"** link, then click **Open** (do not click **Save**)
- g. Click Next at the "Welcome to the Certificate Import Wizard" screen
- h. Click Next at the "File to Import" prompt
- At the "Private Key Protection" screen, check the "Display Password" checkbox, then enter the 16-character password
- j. Verify the password is correct, then click **Next**
- k. At the "Certificate Store" prompt, select "Automatically select the certificate store..." then click Next



- I. At the "Completing the Certificate Import Wizard" screen, click Finish
- m. At the "Import was successful" pop-up, click OK

The recovered key is now installed in the certificate store and ready for use. When opening previously encrypted email, MS Outlook will automatically select the corresponding encryption key from the certificate store to decrypt the message.

MANUAL KEY RECOVERY

When attempting the Automated Key Recovery process, if no encryption keys appear, follow these procedures for the **Manual Key Recovery** process. **NOTE:** This process is for **NIPRNet certificates only**.

- a. Open an Internet browser
- b. Enter the following URL into the web browser:

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

- c. Download and complete the **Key Recovery Request form**, then submit the completed form to the Air Force Key Recovery Agent (AF KRA) via a digitally signed email to: afpki.registration@us.af.mil. Enter "Manual Key Recovery" as the subject
- d. Allow 5-7 business days to process the request (if this is an urgent request, include "**URGENT**" in the subject line and provide justification for the urgency in the body of the e-mail message)

SIPRNET MANUAL KEY RECOVERY

To manually recover SIPRNet encryption keys, obtain the **Key Recovery Request** form from the **SIPRNet AFPKI CoP** or from your issuing Local Registration Authority (LRA). The request should include the Token ID (*i.e., 20-character number located on the back of the token*). **Use a SIPRNet workstation** and your current SIPRNet token to submit the form to the AF KRA via digitally signed, unencrypted email to the AF KRA SIPRNet email address: <u>USAF.JBSA.AFLCMC.MBX.AFPKI.Registration@mail.smil.mil</u>. (*DO NOT SEND THE REQUEST ON NIPRNET*).



NEED ASSISTANCE?

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