MANUAL KEY RECOVERY PROCESS

If no encryption keys appear when attempting the Automated Key Recovery process, follow these procedures for manual key recovery.

a. Open Internet Explorer.

b. Enter the following URL into the Web browser:

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

c. Click the + sign next to Manual Key Recovery Process and follow the instructions

d. Allow 5-7 business days to process the request

Visit the AFPKI SPO Website at:

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

For assistance and additional guidance, contact the AFPKI SPO Help Desk at :

- Phone: 210-925-2521 (DSN 945) or
- Email: AFPKI.helpdesk@us.af.mil

The AFPKI 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

OPR: AFPKI SPO Help Desk
OE-13-01-114
June 2020

AIR FORCE PUBLIC KEY INFRASTRUCTURE SYSTEM PROGRAM OFFICE

CAC REPLACEMENT
SECURE EMAIL USING OUTLOOK 2013-2016

DELIVERING CYBER DEFENSE AND INFORMATION ASSURANCE SOLUTIONS TO THE AIR FORCE

Information in this guide is for CAC holders who have received a replacement CAC

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.

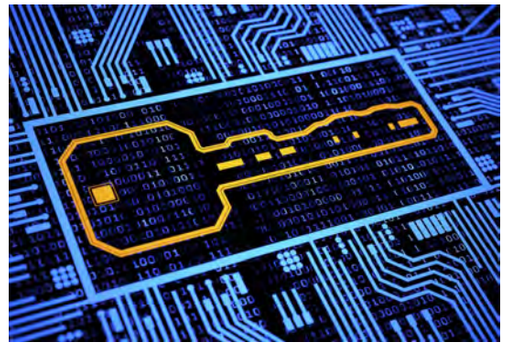
When unclassified e-mail messages are digitally signed and encrypted, they are protected with these PKI assurances:

- 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 your new PKI certificates.

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, 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, insert the CAC into the reader and proceed to Step 1.

Never leave your CAC unattended in the card reader

Step 1: Remove Previous PKI Certificates from IE Certificate Store

a. Insert new CAC in the card reader and open Internet Explorer.

b. Click on the Tools icon at the top right-hand corner, then click Internet Options.

c. Select the Content tab > Certificates button.

d. Select all "old" certificates (CA-31 or higher) with the following exceptions:

DO NOT SELECT

- Previously recovered e-mail encryption certificates *("CN" in the "Friendly Name" column)*
- "Software" Group certificates used for organizational email accounts
- ANY DoD email certificates based on expiration dates only

e. Click the Remove button.

Step 2: Update Outlook Security Profile Settings

a. Remove new CAC from the card reader, then reinsert and open Microsoft Outlook.

b. Click File > Options > Trust Center, then click the Trust Center Settings button *(on the right).*

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. At the "**There is no valid security…**" pop-up, click OK.

g. At the "Your Certificates were removed successfully" pop-up, click OK.

h. Back in the Trust Center, click the Settings button.

i. 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.

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

k. At the warning pop-up, click OK; enter your PIN if prompted.

l. At the **"Your certificates were published successfully"** pop-up, click OK, then click OK to exit the Trust Center *(you may need to restart Outlook).*

Step 3: Recover a Previous Email Encryption Key

Your new CAC contains a new Email Encryption certificate and corresponding encryption key. 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 Internet Explorer.

b. Enter one of the following URLs into the Web browser *(case sensitive):*

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

c. At the **"Window Security"** pop-up, select an Identity Certificate; click OK.

d. Enter your PIN if/when prompted.

e. At the **"Automatic Key Recovery Agent"** page, click I Accept; a list of encryption keys will appear.

f. Based on the date range, select the desired key from the list *(NOTE: the list in not in any order).*

g. Click the blue Recover button.

h. Click I Acknowledge, then click OK.

i. The next screen provides a Download link and a 16-character, case-sensitive password; write the password down EXACTLY as shown.

j. Click on the Download link, then click Open.

k. Click Next at the **"Welcome to the Certificate Import Wizard"** screen *(do not change default buttons).*

l. Click Next at the "**File to Import"** prompt

m. At the **"Private Key Protection"** screen, click the Display Password checkbox, then enter the 16-character password.

n. Verify the password is correct, then click Next.

o. At the **"Certificate Store"** prompt, select Automatically select the certificate store, then click Next.

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

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

r. Click Return to Key List and repeat these steps to recover other Encryption Keys as needed.

The recovered key(s) is/are now installed in the certificate store and ready for use. When opening previously encrypted email, MS Outlook automatically selects the corresponding encryption key from the certificate store.