



# AIR FORCE PUBLIC KEY INFRASTRUCTURE SYSTEM PROGRAM OFFICE

## AUTOMATED KEY RECOVERY E-mail Encryption Certificate/Key

Encrypted e-mail can only be opened with your private encryption key. When your Common Access Card (CAC) is replaced, previously encrypted e-mail messages are not accessible with the new CAC because it contains a new private encryption key.

The Defense Information Systems Agency (DISA) escrows all CAC encryption keys for data recovery purposes. Key Recovery allows you to recover your current or previous encryption key(s), providing continued access to existing encrypted e-mail.

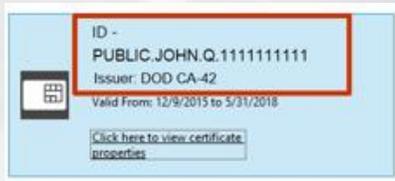
### Procedures to Recover an E-mail Encryption Key

Use these URLs to recover your old encryption certificates:

<https://ara-5.csd.disa.mil>

<https://ara-6.csd.disa.mil>

1. When prompted to choose a certificate, select the **ID** certificate. Using the wrong certificate will direct you to a page stating: "An error has occurred. Please try again in a few minutes."



For more PKI related information please visit the AF PKI Web Site

<https://afpki.lackland.af.mil>

If you need assistance with a PKI-related issue, don't hesitate to contact the AF PKI Help Desk

(210) 925-2521 / DSN 945-2521

E-mail: [afpki.helpdesk@us.af.mil](mailto:afpki.helpdesk@us.af.mil)

DELIVERING CYBER DEFENSE AND INFORMATION ASSURANCE SOLUTIONS TO THE AIR FORCE

HTTPS://AFPKI.LACKLAND.AF.MIL



The AF PKI SPO is part of the Air Force Life Cycle Management Center, Cryptologic and Cyber Systems Division, Engineering Branch, Information Assurance Section (AFLCMC/HNCEI), Joint Base San Antonio - Lackland, TX. Phone: 210-925-2562 / DSN: 945-2562



2. After choosing the ID certificate, type in your **CAC PIN** when prompted. Then click **OK**.

Please enter your PIN.

PIN

\*\*\*\*\*

3. Read the *US Department of Defense Warning Statement (Message from webpage)*, and then click **OK**.

OK

4. You will receive notice that the web site is gathering a list of escrowed keys pertaining to you. It may take a few seconds for the list to appear.



5. The Automated Key Recovery agent should report, "The following Encryption Keys can be recovered" and provide a list of keys to choose from. Review the list of keys to find the serial number and dates (**Not Before / Not After**) that match the timeframe of a desired key – such as the dates of a previous CAC. Click the **Recover** button next to that key.



6. A pop-up window will ask for acknowledgement that you are the DoD subscriber for this escrowed key, click **OK**.

7. The next page will only be available for a couple of minutes. The web page displays a download link and a complex password. Either write down the password (exactly as displayed) or capture a screenshot.



8. After capturing the password, click the DOWNLOAD link to continue with the key recovery.

10. A prompt appears with the choice to either **Open** or **Save** the key. Click **Open** to continue. If you choose the **Save** option, the file must be saved to an approved portable medium, such as a DVD/CD, not to shared online storage.



11. On the *Welcome to the Certificate Import Wizard* screen, click **Next**.

Next >

12. The next prompt indicates the *File to Import*, click **Next**.

Next >

13. Enter the **complex password** copied earlier (bullet# 8), then click **Next**.



14. At the next prompt (*Certificate Store*), select **Automatically select the certificate store...** (default), and then click **Next**.

Automatically select the certificate store based on the type of certificate

15. One the completing the Certificate Import Wizard screen, click **Finish**.

Finish

16. A window stating that the import was successful will display; click **OK**.



17. The key is now installed and ready for use. Outlook will use this key for any e-mail that was encrypted with this recovered key.