DoD PKI
Automatic Key Recovery

(520) 538-8133 or Coml. 866 738-3222,
netcom-9sc.om-iacacpki.helpdesk@mail.mil
Fort Huachuca, AZ 85613-5300
14 March 2017
One problem in the past with the DoD PKI infrastructure was the inability to recover Common Access Card (CAC) private encryption keys and certificates that were either expired or revoked. This becomes necessary when a CAC is lost and its certificates are revoked or when a CAC and the certificates it contains simply expires and is surrendered to DEERS/RAPIDS before the user’s encrypted emails have been decrypted.

An Auto Key Recovery capability has been fielded by DISA to permit holders of new CACs to retrieve encryption keys/certificates from previous cards to permit decryption of old email.
The following slides identify steps to recover private encryption keys, escrowed by DISA, from CACs that do not have the “Auto Key Recovery” functionality.
You must use Firefox or Chrome to recover keys. Internet Explorer does not seem to work consistently.

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

SIPR:
https://krp.csd.disa.smil.mil/krp/ss/selfService.jsp

These are the Automatic Key Recovery URLs. They can only be accessed from the .mil network (NIPRNet). TLS 1.1 and 1.2 MUST be enabled.

Note: The URL addresses shown above are case sensitive.

When you go to this link, you must identify yourself with PKI credentials. Use ONLY your identity certificate!
At this time open the URL

**NIPR:**

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

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

**SIPR:**

https://krp.csd.disa.smil.mil/krp/ss/selfService.jsp

Note: You may have to go to all four URLs listed and download all keys available that are four years old or newer to get the correct key to decrypt emails. If that fails, look at the instructions listed on slides 28 and 29.
You will be prompted to identify yourself.

Highlight your Identification Certificate from your CAC. Select it by clicking “OK”.

Note: Do NOT choose any that contain the word “EMAIL” from the Issuer column.
Dismiss the warning by clicking “I Accept”.
Browse through the list and locate the appropriate key you want to recover. When located, click the adjacent associated “Recover” button.
Select “OK”.

Acknowledgement of DoD Subscriber
This is your one-time PIN to install your Private Encryption Key.
You will be given the opportunity to install the certificate, select “Open With” and then click “OK”.

Opening NOBLE.PHILIP.EUGENE.1184204718.p12

You have chosen to open:

- NOBLE.PHILIP.EUGENE.1184204718.p12
  which is: p12 File
  from: https://ara-5.csd.disa.mil

What should Firefox do with this file?

- Open with
- Save File
- Do this automatically for files like this from now on.
Installing the Certificate (Cont’d)

Click “Next”.
Installing the Certificate (Cont’d)

Click “Next”.
Check the blocks as shown, enter your Password, and click “Next”.
Ensure that "Automatically select the certificate store based on the type of certificate" is selected (as shown above) and click “Next”.

Ensure that “Automatically select the certificate store based on the type of certificate” is selected (as shown above) and click “Next”. 
Installing the Certificate (Cont’d)

Click “Finish”.
Click “OK”
Click “OK”.

The import was successful.
Select “Logout” in the top-right corner
Successful Logout

Close the browser window
Medium Security is Not a Choice

If Medium Security is blocked and High Security is default, refer to:

Use gpedit.msc:
- Local computer policy
  - Windows settings
    - Security settings
      - Local policies
        - Security options

Temporarily set - **System Cryptography: Force Strong Protection for User Keys Stored on the Computer to User Input is Not Required When New Keys are Stored and Used**

After the key is imported, change the setting to – **User Must Enter a Password Each Time They Use a Key**
From MEPCOM:

During the process of importing the certificate, the user receives the following Password Error no matter what password is entered: ‘The password supplied does not meet the minimum complexity requirements’. Almost simultaneously the following error appears: ‘Windows has encountered a critical problem and will restart automatically in one minute’. The error condition has also been encountered during the process of attempting to recover email certificates. In many cases, local security policies may not allow the use of ‘Medium Security’ from the previous page.
Importing The Recovered Key

Solution: The enpasflt.dll is in use and must be unloaded to correct the issue. Log into the computer using an account with administrative rights to complete the following:

• Click Start | Type regedit | Press Enter
• Navigate to HKLM\System\CurrentControlSet\Control\LSA | Navigate to Notification Packages in the right pane
• Remove the enpasflt entry | Ensure that the scecli entry remains
• Restart the computer

Note: After the certificates have been loaded or recovered, you will need to re-install the EnPasFIt

• Navigate to C:\Windows\AGMSupport\EnPasFIt
• Double Click Installer.exe

Note: This install is silent and applies immediately

• Open regedit
• Navigate to HKLM\System\CurrentControlSet\Control\LSA\Notification Packages
• Ensure that the enpasflt entry is present
• Close regedit
Close the open window, you may now use the recovered key to access your encrypted email.

Last Step: If you chose to save the recovered key to a file instead of directly installing the key, delete the saved .P12 file from your computer as this is a security vulnerability and will be detected in a Q-tip Scan. Disregard if you did not save the key to a file.

Should recovery fail, contact the Army Key Recovery Agent by sending a signed email to:

usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil

Send the digitally signed email requesting recovery of old PKI encryption certificates and provide the following:

1. Your name and by your name your 10 digit EDIP (ex. Doe.John.1234567890)
2. The CA certificate was issued on (ex. CA20)
3. The serial number (ex. 0x12fA3).
4. Also please provide the exact reason for having to recover your keys.
5. The key(s) you need recovered.
Other Services

Navy Key Recovery Agent
https://infosec.navy.mil/PKI/
NCMS_NAFW_NAVY_RA@navy.mil
Phone: 800-304-4636
DSN 588-4286

USMC RA Operations Helpdesk
Email: raoperations@mcnosc.usmc.mil
Phone: 703-432-0394

Air Force PKI Help Desk
Phone: 1-210-925-2521
Email: afpki.ra@lackland.af.mil
https://afpki.lackland.af.mil/html/lracontacts.asp (this site is accessible from .mil domains only)
Additional Air Force PKI support is available from the Air Force PKI help desk:

DISA PKI Help Desk Oklahoma City, OK Support:
E-Mail: disa.tinker.eis.mbx.okc-service-desk@mail.mil
1-844-347-2457, then select options 1, 5 and 4 in that order