DoD PKI
Automatic Key Recovery

Adam Simmons
(520) 538-8133, DSN 312-879-8133, or 866-738-3222,
Netcom-9sc.om-iacacpki.helpdesk@mail.mil
Fort Huachuca, AZ 85613-5300
17 November 2015

Mike Danberry last reviewed on 17 November 2015
http://militarycac.com/questions.htm

The most current version of this guide can be downloaded from:
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 / files 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 and files.

NOTE: Please know that in April 2014, DISA changed the links for recovery to ONLY be available from the unclassified Government network. You’ll need to follow instructions on slides 23 for Army users & 24 for all other military branches to get your former CAC certs for home users.
The following slides identify steps to recover private encryption keys, escrowed by DISA, from previously held CACs.
The links listed below are ONLY available from the Government UnClassified network, NOT from a personal computer at home.

NOTE: TLS 1.0, 1.1, & 1.2 must be checked on your Government computer in Internet Explorer, Tools, Internet Options, Advanced (tab)

https://ara-1.c3pki.chamb.disa.mil/ara/Key
Or
https://ara-2.c3pki.den.disa.mil/ara/Key
Or
https://ara-3.csd.disa.mil/ara/Key
Or
https://ara-4.csd.disa.mil/ara/Key

Note: The links shown above ARE case sensitive

You may have to visit all four URLs listed to get your keys. If the keys fail in all links, follow instructions on slides 23 for Army users & 24 for all other military branches.
Choose Your Identity Certificate

When prompted to identify yourself, Highlight your Identification Certificate. Select it, then click OK.

Note: Do NOT choose the EMAIL or PIV certificates
Read the warning message, then click **OK**
The Automated Key Recovery Agent will compile a list of Recoverable Keys. If the recovery fails or if the key is unable to be downloaded automatically, contact the Army Key Recovery Agent by sending a digitally signed email to: usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil requesting recovery of your private email encryption Key.

DO NOT click the Logout button on this screen.
Browse through the list and locate the appropriate key you want to recover. When located, click the adjacent associated Recover button.

Hint: Look for the dates that correspond with your former CAC. They may not be listed in order.
Acknowledgement of DoD Subscriber

Select OK
The Automated Key Recovery Agent is processing your request.

Do NOT be tempted to click the Logout button, you Must Wait.
Click the DOWNLOAD… link, you’ll need the one-time password to access your Private Encryption Key
Installing the Certificate

Select **Open**
Installing the Certificate (Cont’d)

Click Next
Installing the Certificate (Cont’d)

Click Next
Installing the Certificate (Cont’d)

Enter the Password shown on web page, leave the blocks unchecked, click Next
Installing the Certificate (Cont’d)

Leave “Automatically select the certificate store based on the type of certificate” selected  click Next
Installing the Certificate (Cont’d)

Click *Finish*
Click OK
Click **OK**
Verify the successful download of your recovered Private Encryption Key by: Launching Internet Explorer, selecting *Tools* from the menu, and then *Internet Options*. Click the *Content* (tab) then *Certificates* (button).
Select the *Personal* (tab) you’ll see a list of your currently registered certificates, including the recovered key certificate(s).
Double-click on the certificate so you can view the specifics of your recovered key (or other current keys) as illustrated above.
Close the open window, you may now use the recovered key to access your encrypted email.

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

Remember if the recovery failed, Army users, contact the Key Recovery Agent by sending a digitally signed email to:

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

requesting recovery of your private email encryption key

All other military branches look at slide 24
Other Services

SPAWAR Integrated Support Center Helpdesk
https://infosec.navy.mil/PKI/
Email: itac@infosec.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: 210-925-2521
Email: afpki.ra@lackland.af.mil
https://afpki.lackland.af.mil/html/lracontacts.asp  (this site is accessible from .mil networks 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: Okc-dodost@csd.disa.mil
Phone: 800-490-1643
          Phone (DSN): 312-339-5600
A user has attempted to recover a key using the Automated Key Recovery Agent. The ID Certificate used for Authentication was:
CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0B5643, Issuer: DOD CLASS 3 CA-5. The key that was recovered was:
CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0C8747, Issuer: DOD CLASS 3 EMAIL CA-3.

If you did not perform this operation, please contact your local key recovery agent and ask that they check the logs for the key recovery at Fri Jul 01 16:48:12 GMT 2005 with session ID 1.c3pki.chamb.disa.mil-23f%3A42c57335%3A68e46e9395fb9727.

You will receive an email from PKI_ChambersburgProcessingElement@csd.disa.mil with a subject “ALERT! Key Recovery Attempt Using Automated Key Recovery Agent” similar to the above Recovery Notification example notifying you of your recovery action.
POC for Additional Information

Philip E. Noble
USAISEC
Information Assurance and Security Engineering Directorate (IASED)
DSN 312-879-7608
CML 520-538-7608
FAX DSN 312-879-8709 CML 520-538-8709
philip.e.noble.civ@mail.mil
philip.e.noble.civ@mail.smil.mil