

YOU'VE BEEN ISSUED A NEW CAC, HERE IS WHAT YOU SHOULD DO NEXT...

Recovering old encryption keys

When you replace or renew your common access card (CAC) or Public Key Infrastructure (PKI) certificates, you acquire a new encryption key. The new encryption key cannot open email messages that were encrypted with your previous encryption keys. To read messages encrypted with your previous encryption keys, download your previous encryption keys from one of the Defense Information Systems Agency (DISA) Automated Key Recovery Agent (ARA) sites and install them on your workstation:

Below are the websites available to recover your email certificate when you get a new CAC:

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

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

<https://ara-3.csd.disa.mil/ara/Key>

*If the first website doesn't work for you then select the second one; if that one doesn't work either then select the last website. One out of the three websites should work.

Publishing Certificates to the GAL (Send/Receive Encrypted Emails)

- In Outlook, select 'File' and then 'Options'
- Select 'Trust Center' then 'Trust Center Settings'
- Select 'E-mail Security' and then 'Settings'
- Under Certificates and Algorithms, select 'Choose..' next to Signing Certificate'
- Select your DOD CA-## certificate and press OK
- Select 'Choose...' next to 'Encryption Certificate'
- Select your DOD EMAIL CA-## Certificate and press OK
- Select OK to close out of screen
- Select 'Publish to GAL..' to update (You may need to enter in your PIN)
- You should now be able to send/receive encrypted emails