DoD PKI
Automatic Key Recovery

(520) 538-8133, DSN 312-879-8133, or 866-738-3222,
Netcom-9sc.om-iacacpki.helpdesk@mail.mil
Fort Huachuca, AZ 85613-5300
14 March 2017

Mike Danberry last reviewed on 26 April 2021
https://militarycac.us/questions.htm

The most current version of this guide can be downloaded from:
https://militarycac.us/files/Automatic_Key_Recovery_New.pdf

The Problem:

A 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 expires and is surrendered to DEERS / RAPIDS site 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: In April 2014, DISA removed the Certificate recovery website "white listing," changing the site to <u>ONLY be available from the UnClassified Government network</u>. Home users will need to follow instructions on slide 21 for Army users & 22 for all other military branches to get your previous CAC certificates. ***See slide 24 for another idea if you have access to a Government computer***

The Solution:

Steps to Recover CAC Private Email Encryption Keys

The following slides provide steps to recover private encryption keys [escrowed by DISA] from your previously CACs

URLs for Key Recovery

The links listed below are <u>ONLY</u> accessible from the Government UnClassified network

<u>They will NOT work</u> from a personal computer at home

<u>TLS 1.0, 1.1, & 1.2</u> must be checked on your Government computer in Internet Options, Advanced (tab). ***Some Government computer users may have to use Firefox, as their commands have blocked the ability to check TLS 1.0, 1.1, & 1.2***

NOTE: Some people have had better success using Firefox or Chrome

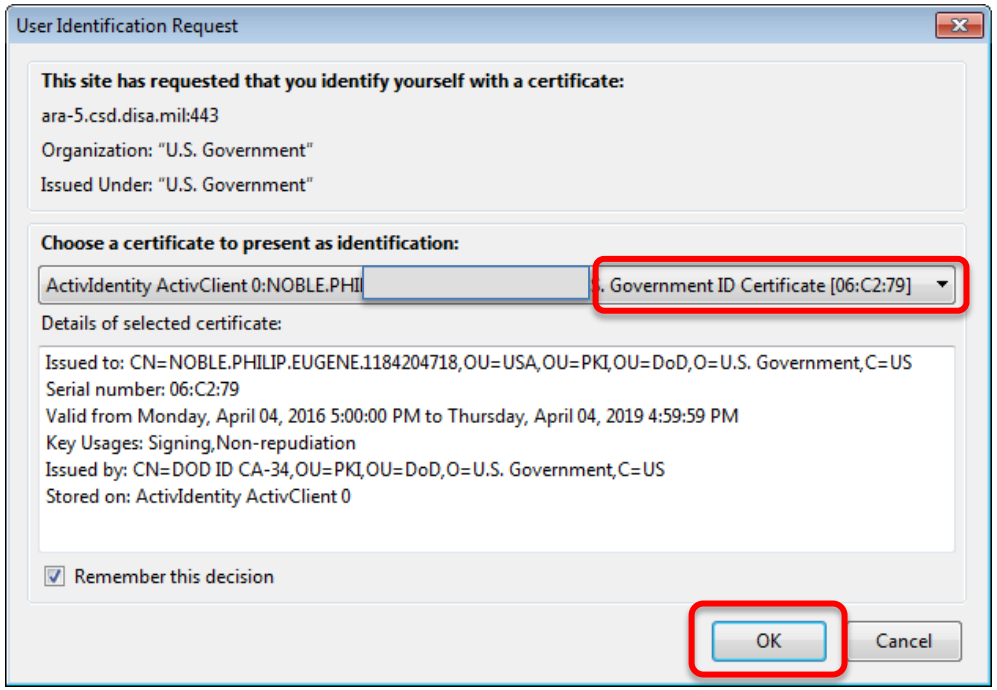
https://ara-5.csd.disa.mil or https://ara-6.csd.disa.mil

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

Note: <u>The links shown above ARE case sensitive</u>

If the keys fail in the links, follow instructions on slide 21 for Army users & 23 for all other military branches.

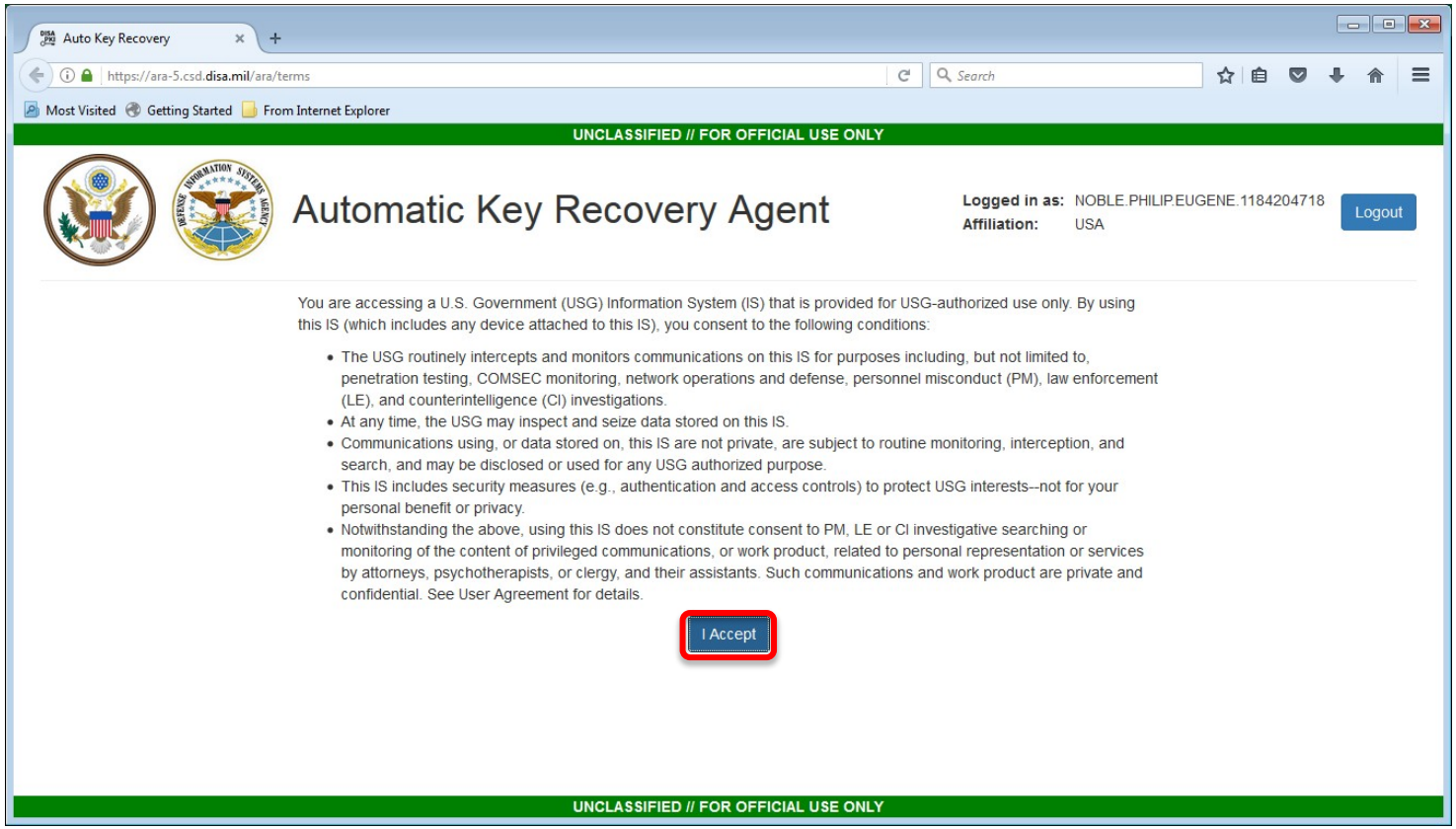
Choose Your Identity or Authentication Certificate



When prompted to identify yourself, Highlight <u>your</u> Identification Or Authentication Certificate. Select it, then click *OK*.

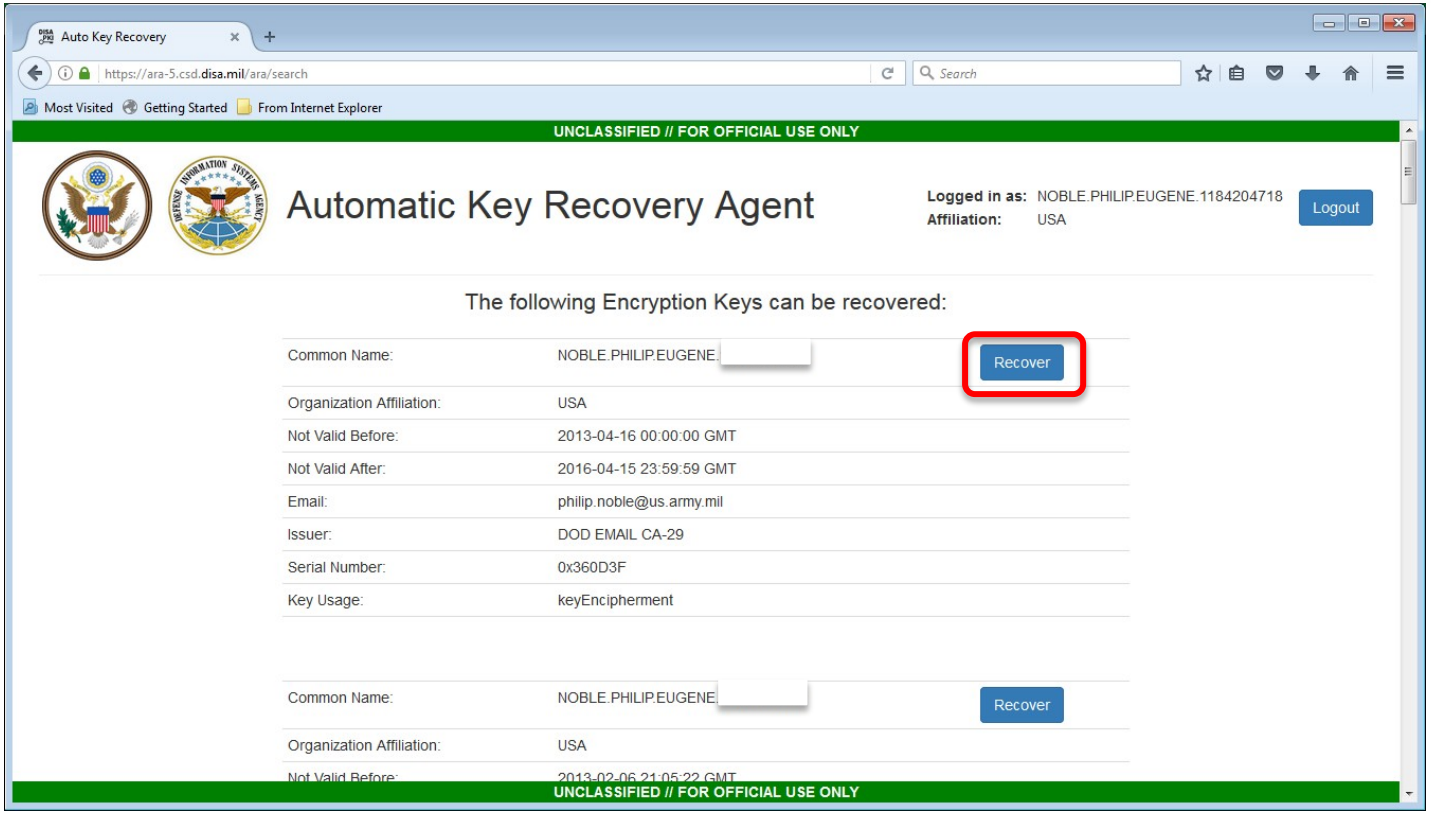
Note: <u>Do NOT</u> choose the <u>EMAIL</u> certificate

Warning Banner



Read the warning statement, then click *I Accept*

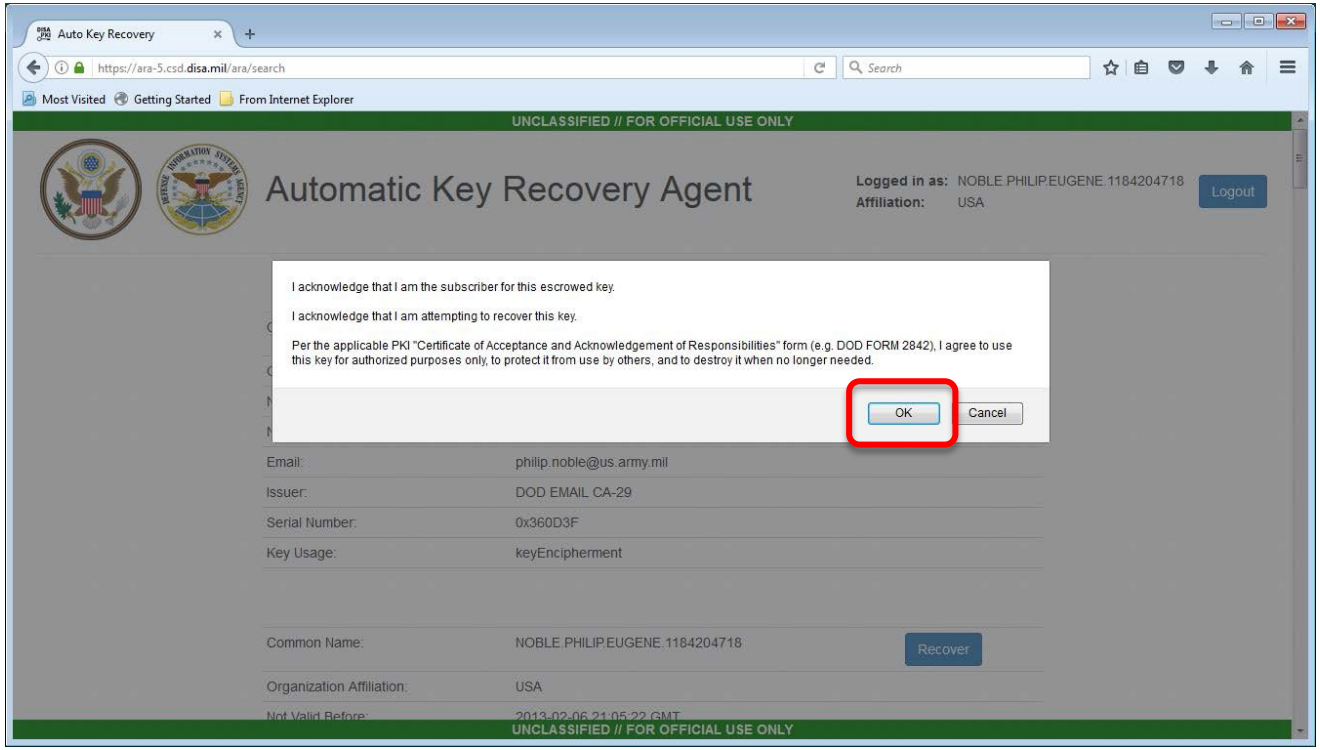
Key Selection



Look for the dates that correspond with your <u>previous</u> CAC(s). They may not be listed in order. Only recover previous certificates. There is no need to recover your current CAC certificate

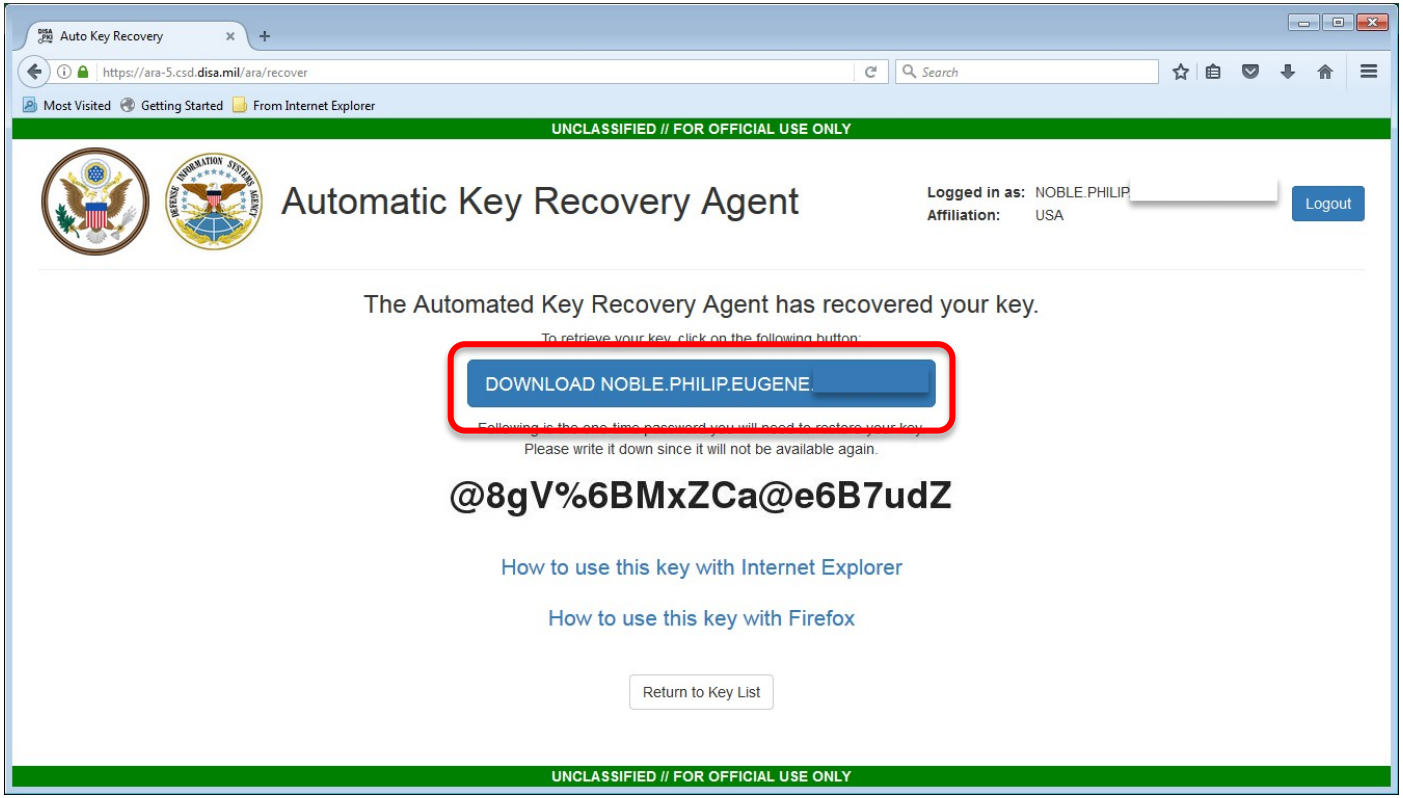
Browse the list and locate the key you want / need to recover. Once located, click the *Recover* button.

Acknowledgement



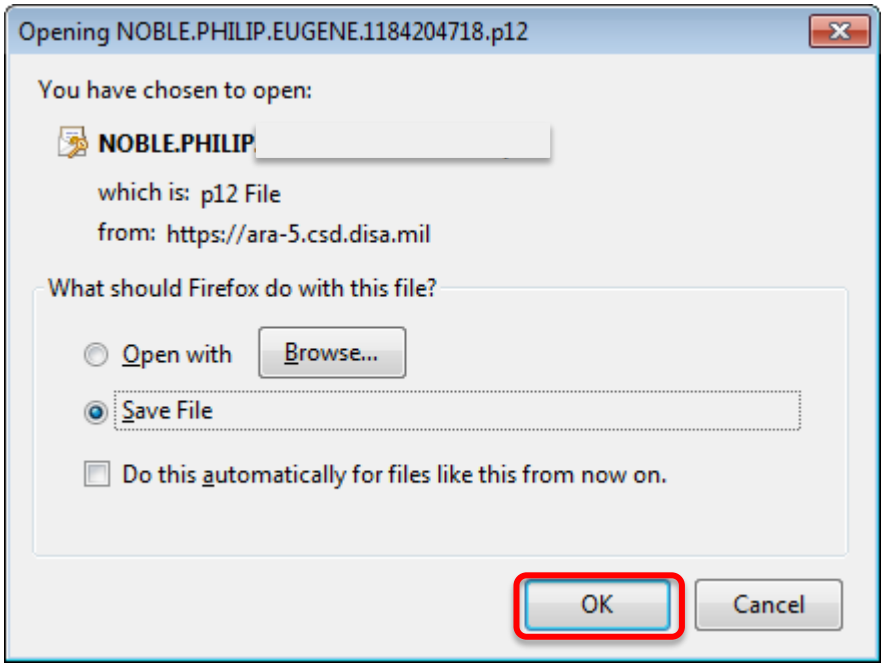
Select *OK*

One-time Password



Click the DOWNLOAD (button), you'll use the one-time password to access / install your recovered certificate

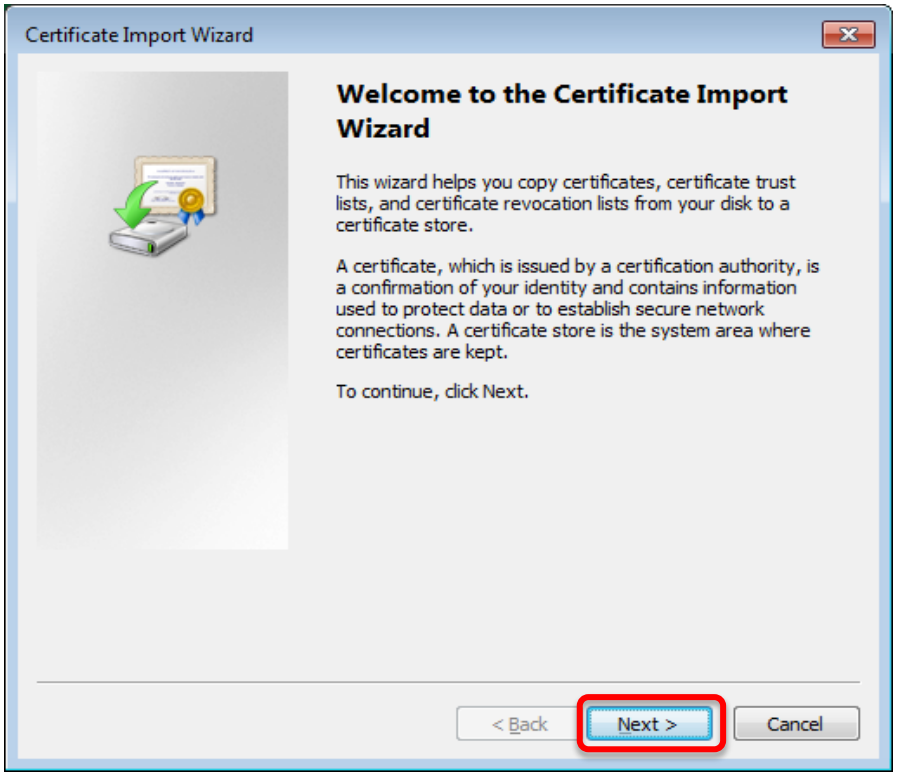
Installing the Certificate



Select *OK*

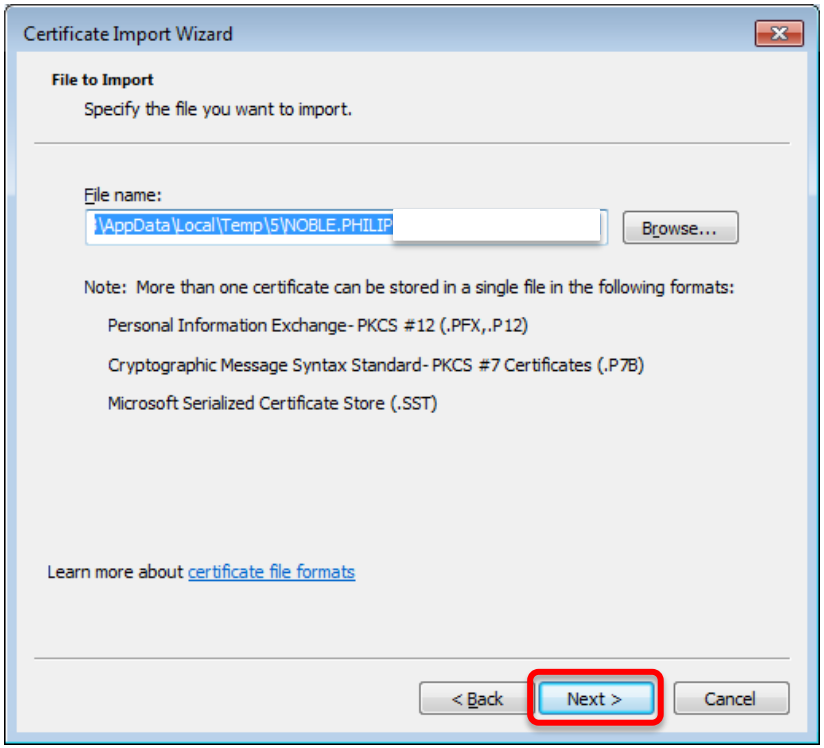
People following slide 24, select *Save*, then after you get home continue with this guide by clicking *Open*

Installing the Certificate (Cont'd)



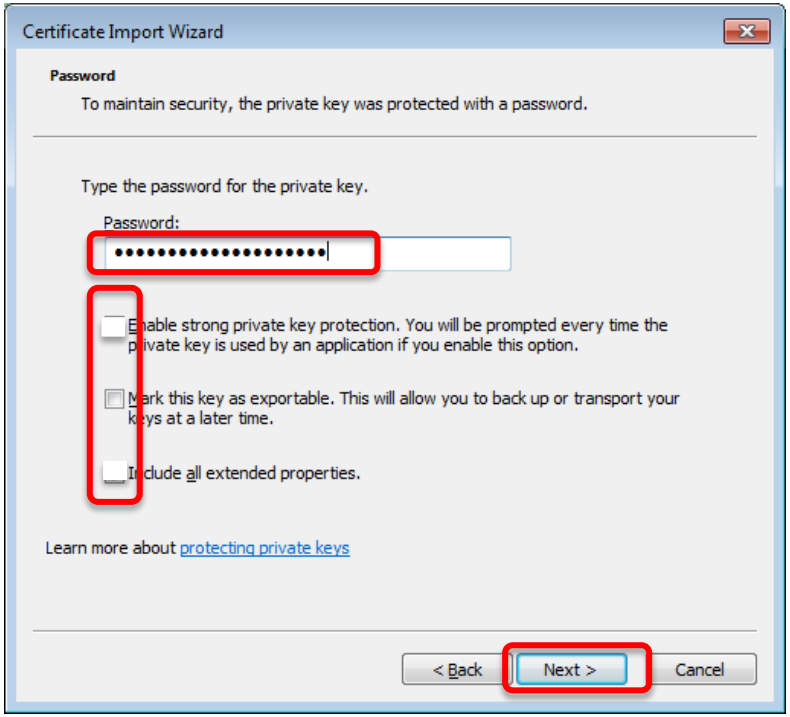
Click *Next*

Installing the Certificate (Cont'd)



Click *Next*

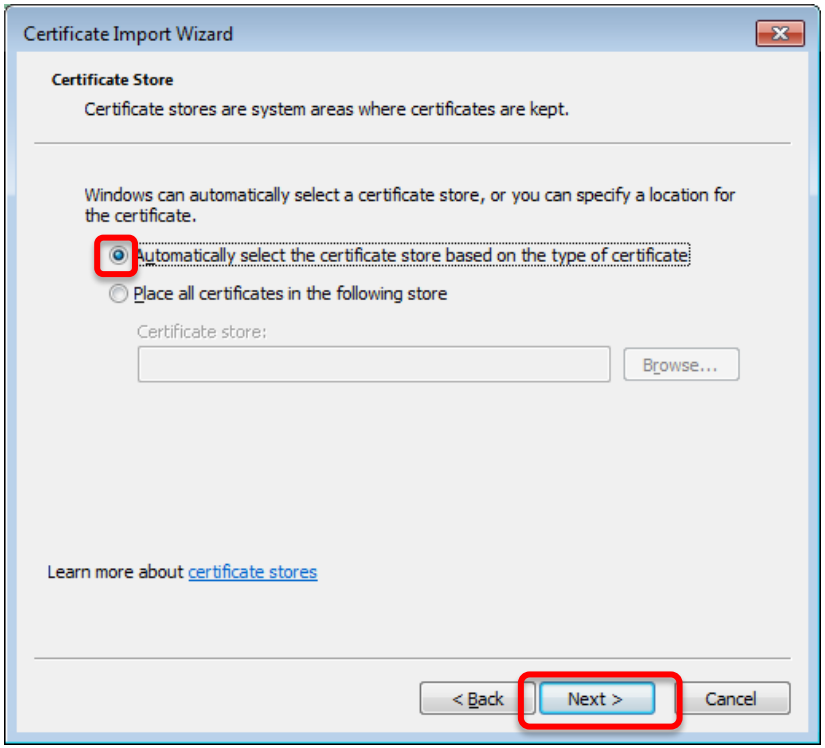
Installing the Certificate (Cont'd)



Note: If you check "Enable strong private key protection" you'll need to enter the password provided every time you access your email / files. So, recommendation is to NOT check it.

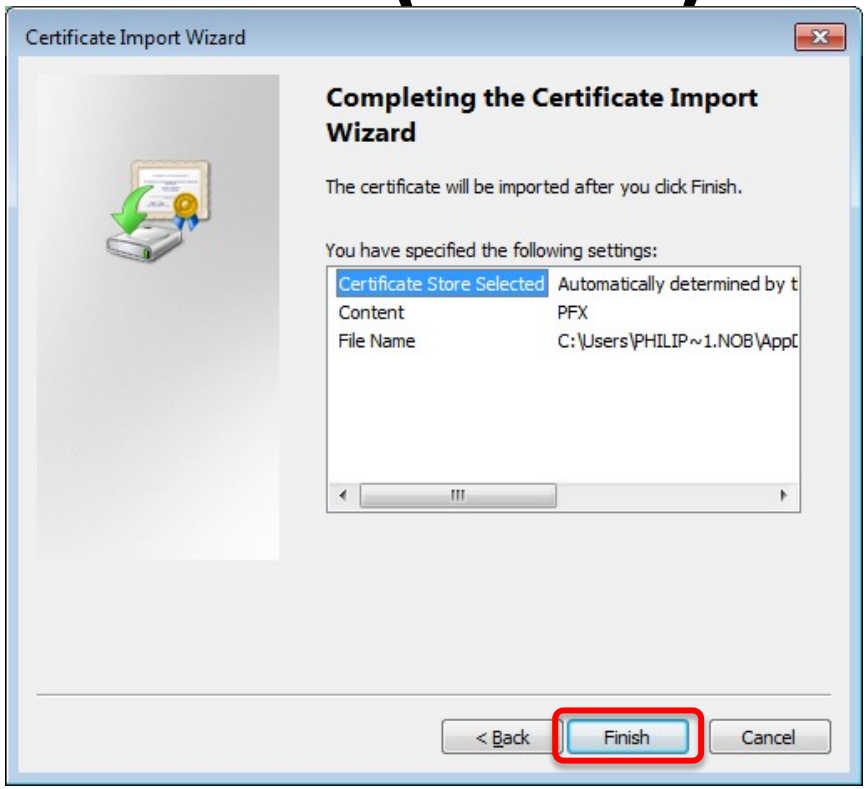
Enter the Password shown on the download link web page, leave the blocks unchecked, click *Next*

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)

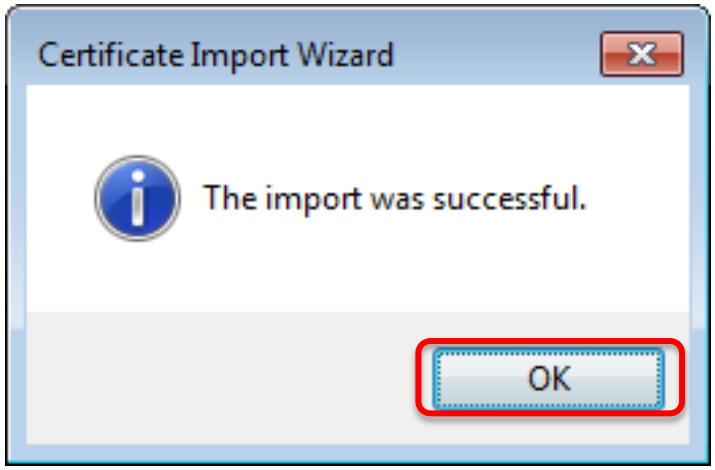


Click *Finish*

Installing the Certificate (Cont'd)

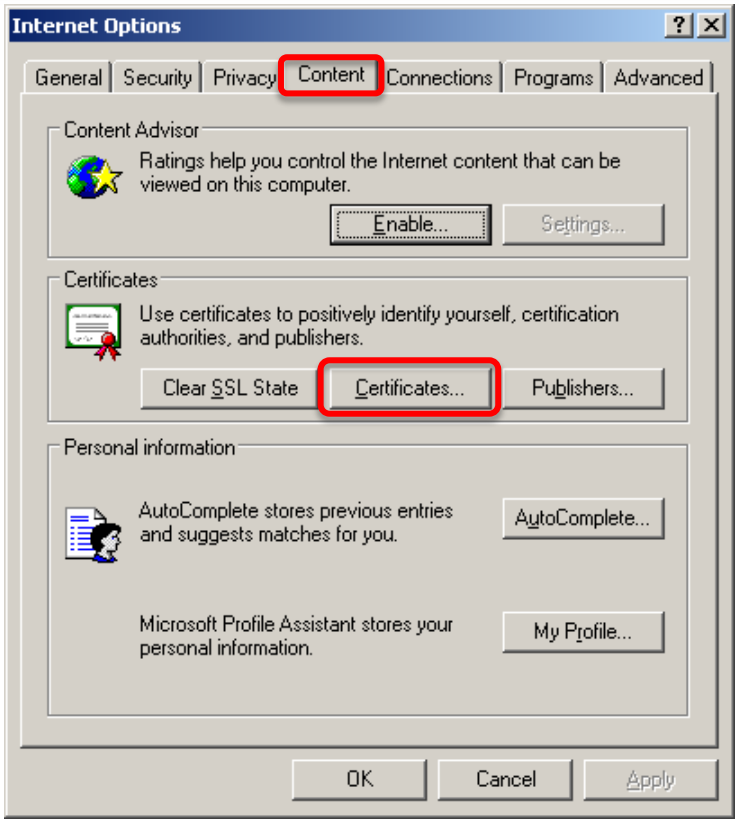
Click *OK*

Installing the Certificate (Cont'd)



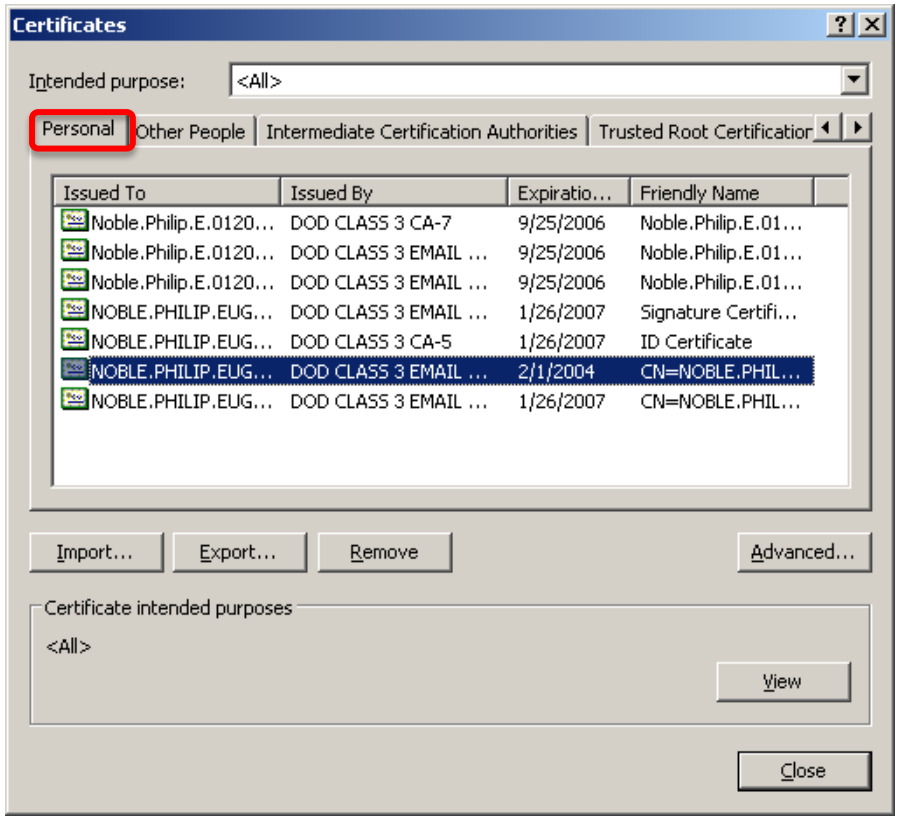
Click *OK*

Verifying the Download



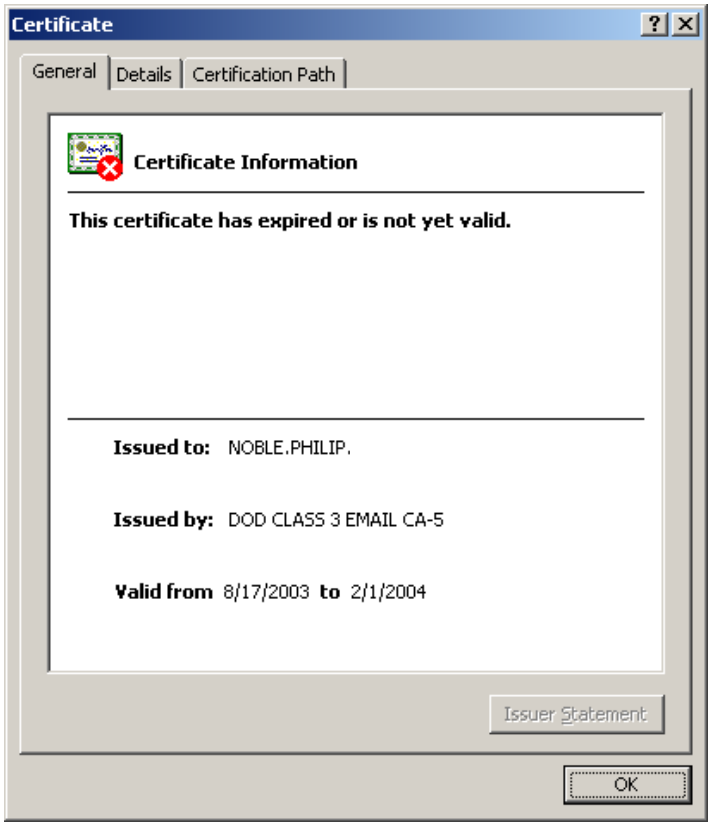
Verify the successful download of your recovered certificate by: Launching Internet Explorer, selecting *Tools* from the menu, *Internet Options, Content* (tab), *Certificates*… (button)

Verifying the Download (Cont'd)



Select the *Personal* (tab) to see a list of your currently registered certificates, including the recovered key certificate(s).

Verifying the Download (Cont'd)



Double-click the certificate to view the specifics of your recovered key (or other current keys).

Success

Close the open window, you may now use the recovered key to access your encrypted email.

Last Step: If you saved the recovered certificate to your computer instead of directly installing it, you need to delete the .P12 file. This is a security vulnerability and could be detected in a scan. Disregard if you did not save the certificate to your computer

If the recovery failed, Army users, contact the Key Recovery Agent by sending a digitally signed email from your DoD Enterprise Email account to: usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil requesting recovery of your private email encryption key

Send your digitally signed email requesting recovery of old PKI encryption certificates and provide the following (you'll get this information from the page shown on slide 8):

1. Your name and 10 digit DoDID [on back of your CAC] (ex. Doe.John.J.1234567890)
2. The CA certificate (ex. CA-32)
3. The serial number (ex. 0x12fA3)
4. Provide exact reason why you are recovering your certificate(s)
5. The certificates you need recovered

Other Services

Navy Key Recovery Agent
https://infosec.navy.mil/PKI/
Email: NCMS_NAFW_NAVY_RA@navy.mil
Phone: 800-304-4636
DSN 312-588-4286

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:
https://afpki.lackland.af.mil/html/help_desk.asp

DISA PKI Help Desk Oklahoma City, OK Support:
E-Mail: disa.tinker.eis.mbx.okc-service-desk@mail.mil
Phone: 844-347-2457, Options: 1, 5, 4

Recovery Notification Email Example

A user has attempted to recover a key using the Automated Key Recovery Agent. The ID Certificate used for Authentication was:
CN=NOBLE.PHILIP. ,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. ,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.

Home users needing their certificates to open old emails in webmail

Reminder [mentioned on slide 2] in April 2014, DISA removed the Certificate recovery website white listing, changing the site to ONLY be available from the UnClassified Government network. This put home users in an unfortunate situation as you may need to access old encrypted emails via OWA.

An idea for you [if you have access to a Government computer], is to follow slides 4-10, save the file(s) to the computer you are on, and not run it. When you get to slide 9, type the password into a .txt file or into an email to yourself using DoD Enterprise Email. Attach the .p12 file to the email and save it to your drafts. Do not email it. You are merely "holding" it there until you get home. Once you are home, continue with slides 11-20 using the password you included in your email. It will install into your certificate store, and you should be able to open up your former encrypted emails.