



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

24 August 2016

Mike Danberry last reviewed on 11 May 2017

<http://militarycac.us/questions.htm>



**The most current version of this guide can be downloaded from:
[http://militarycac.us/files/Automatic Key Recovery New.pdf](http://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 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 removed the Certificate recovery website "white listing," changing the site to ONLY be available from the Unclassified Government network. Home users will need to follow instructions on slide 23 for Army users & 24 for all other military branches to get your previous CAC certificates. *See slide 26 for another idea.*



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 held CACs



URLs for Key Recovery



The links listed below are ONLY available from the Government UnClassified network, NOT from a personal computer at home

TLS 1.0, 1.1, & 1.2 must be checked on your Government computer in Internet Explorer, Tools, 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*

CA 32 and below <https://ara-3.csd.disa.mil/ss> (currently NOT Working)

CA 33 and up <https://ara-5.csd.disa.mil> or <https://ara-6.csd.disa.mil>

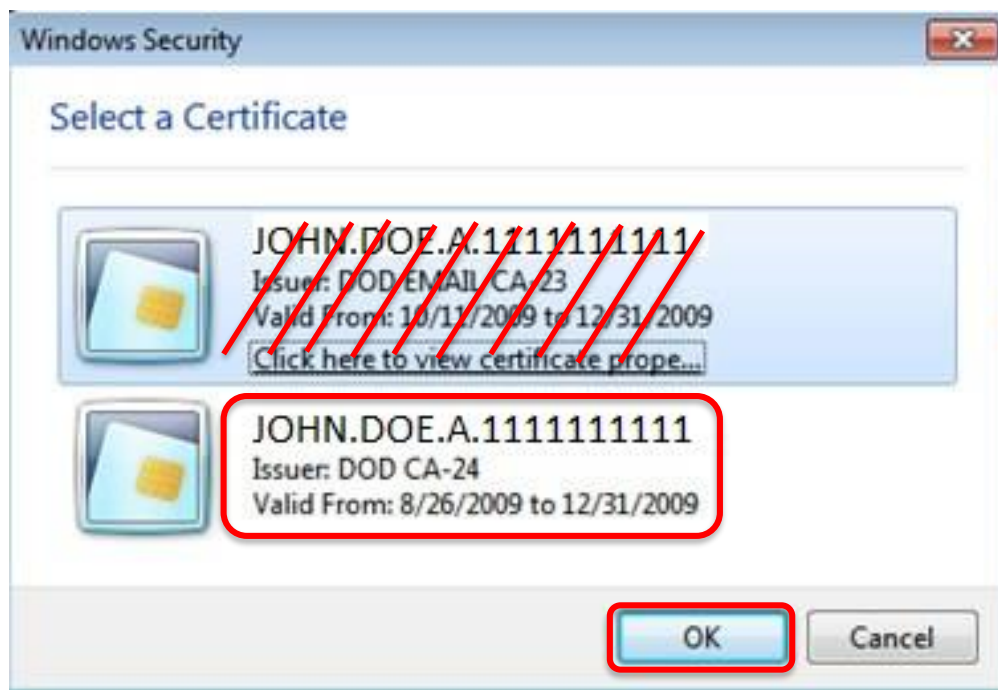
SIPR users: <https://krp.csd.disa.mil/krp/ss/selfService.jsp>

Note: The links shown above ARE case sensitive

If the keys fail in the links, follow instructions on slide 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



Warning Banner



The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `https://ara-1.c3pki.chamb.disa.mil/ara/Key`. The page content includes the Defense Information Systems Agency logo and the text "Automated Key Recovery For Official Use Only". A "Please Wait." message is displayed on the page, along with a "Log in" button. A warning dialog box is overlaid on the page, containing the following text:

Microsoft Internet Explorer

Warning

US Department of Defense Warning Statement: This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject the user to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

OK

Read the warning statement, then click **OK**



Processing Your Request

click here'. A 'Logout' button is visible at the bottom left of the page content."/>

Auto Key Recovery - Wait for Recoverable Key List - Microsoft Internet Explorer

Address <https://ara-1.c3phi.chamb.dsa.mil/araKey>

DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions... The Warfighter's Edge

Automated Key Recovery
For Official Use Only

Please Wait.

The Automated Key Recovery Agent is gathering a list of Recoverable Keys for you.
This process can take up to one minute.
Please do not hit the "Back" button on your browser toolbar.

If the list does not appear within one minute, please [click here](#)

Logout

You have to Wait on this screen, DO NOT click the Logout button

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 following guidance on slide 23 or slide 24 for all other military branches.



Key Selection



The screenshot shows a web browser window titled "Auto Key Recovery - Recoverable Key List - Microsoft Internet Explorer". The address bar shows the URL: <https://ara-1.c3pki.chamb.disa.mil/ara/Key?value=96287>. The page header includes the Defense Information Systems Agency logo and the text "DEFENSE INFORMATION SYSTEMS AGENCY Global Net-Centric Solutions - The Warrior's Edge". Below the header, the page is titled "Automated Key Recovery" with a sub-header "For Official Use Only". The main content area displays a list of encryption keys that can be recovered. Each entry includes the following fields: Common Name, Organization Affiliation, Not Before, Not After, Email, Issuer, Serial #, and Revocation Status. The first entry has a "Recover" button. The second entry has a "Recover" button, and its "Not Before" and "Not After" dates are highlighted with a red box. The third entry has a "Recover" button.

Common Name	Organization Affiliation	Not Before	Not After	Email	Issuer	Serial #	Revocation Status	Action
NOBLE.PHILIP.	USA	2002-04-29 00:00:00 GMT	2005-04-28 00:00:00 GMT	philip.noble@us.army.mil	DOD CLASS 3 EMAIL CA-4	0x05DCF3	REVOKED	Recover
NOBLE.PHILIP.	USA	2004-01-28 00:00:00 GMT	2007-01-27 00:00:00 GMT	philip.noble@us.army.mil	DOD CLASS 3 EMAIL CA-5	0x0DD98B		Recover
NOBLE.PHILIP.	USA	2003-08-18 00:00:00 GMT	2004-02-02 00:00:00 GMT	philip.noble@us.army.mil	DOD CLASS 3 EMAIL CA-5			Recover

Look for the dates that correspond with your previous CAC(s). They may not be listed in order. Some seem to think they need to recover their current CAC, you need previous certificates

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



Acknowledgement



Select *OK*



Processing Request



DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions - The Warfighter's Edge

Automated Key Recovery
For Official Use Only

Please Wait.

The Automated Key Recovery Agent is recovering the key you selected.
This process can take up to two minutes.

Please do not hit the 'Back' button on your browser toolbar.

If the results do not appear within two minutes, [click here](#)

Logout

The Automated Key Recovery Agent is processing your request

DON'T click the Logout button, you Must Wait



One-time Password



Auto Key Recovery - Recovered Key - Microsoft Internet Explorer

Address <https://ara-1.c3pki.chamb.disa.mil/ara/Key?value=57466>

DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions - The Warfighter's Edge

Automated Key Recovery
For Official Use Only

The Automated Key Recovery Agent has recovered your key.

To retrieve your key, select the following link:

[NOBLE.PHILIP.](#) [DOWNLOAD](#) [_0x01B42B5_DOD_E_CA-](#)
[12](#)

Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.

9Gh2rk3Pazfird#X

To restore your key to your Internet Explorer browser, perform the following steps:

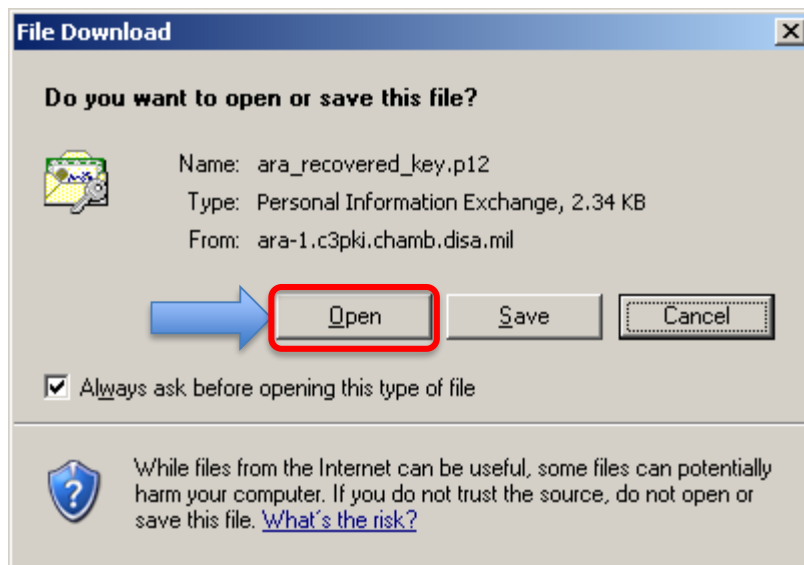
- 1) The Recovered Key will be automatically presented to your browser. You can choose to either save the key to your file system, or open it. If you choose to save it, you can later import the key to your browser using the toolbar 'Tools->Internet Options', select the 'Content' tab and 'Certificates' button, and press 'Import'. Then follow the instructions below.
- 2) In Wizard, select Next, if opening from file Browse to the filename and Select Next.
- 3) Enter the password as displayed when your recovered key was returned to you and then Next.
- 4) Leave the 'Automatically Select the Certificate Store' selected, unless you have other needs.
- 5) Press 'Finish', and your key will appear in your browser keystore.

https://ara-1.c3pki.chamb.disa.mil/ara/Key/NOBLE.PHILIP.EUGENE.1184204718__0x01B42B5__DOD_E_CA-12.p12

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



Installing the Certificate

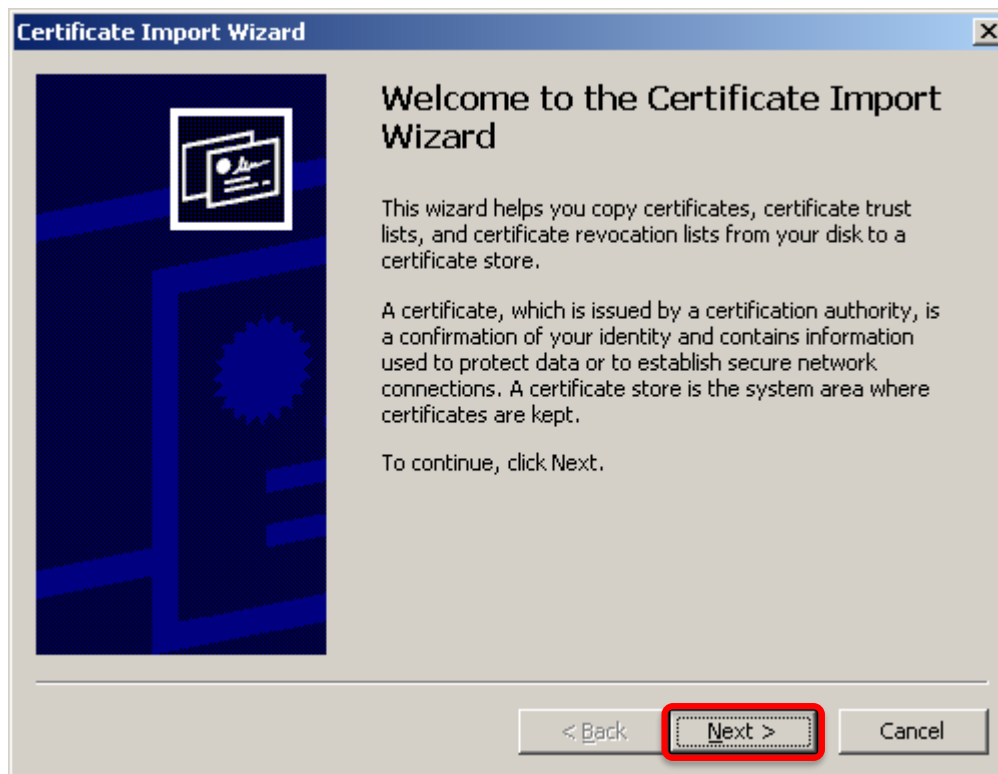


Select *Open*

People following slide 26, select *Save*, then after you get home continue with this guide by clicking *Open*



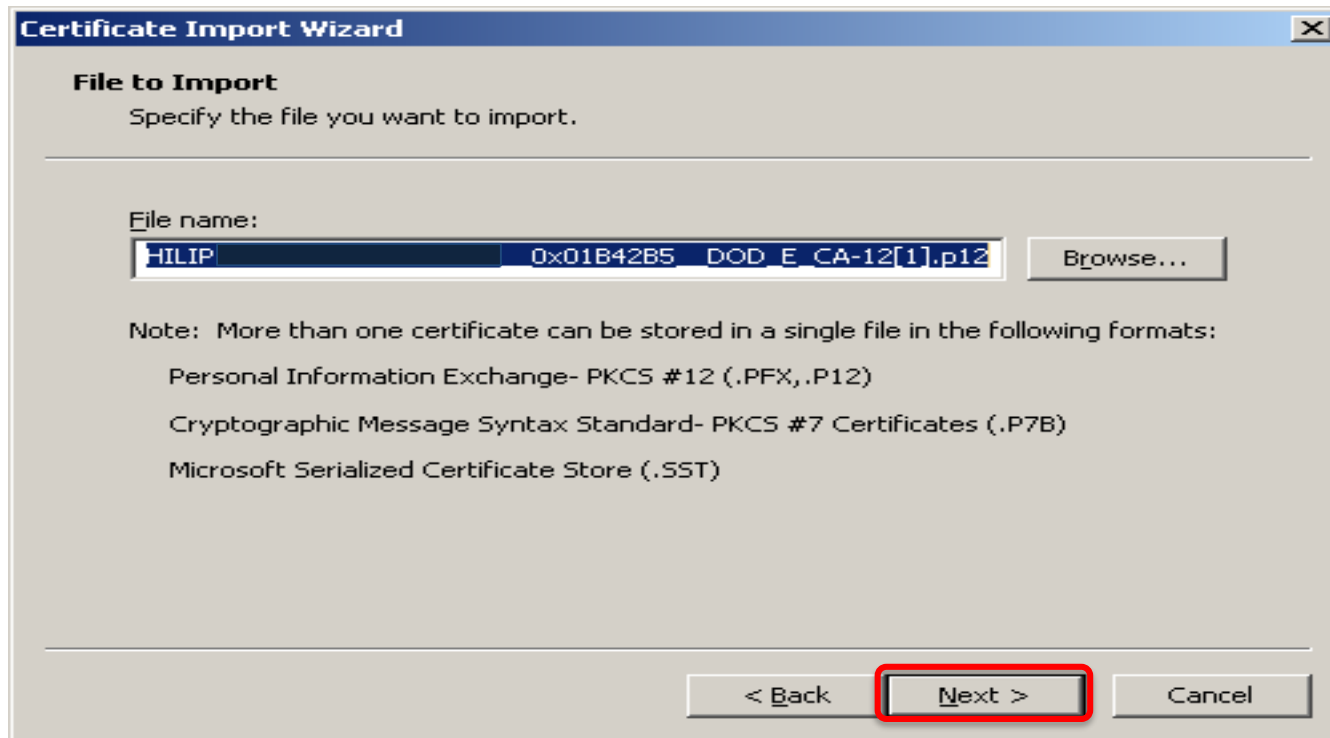
Installing the Certificate (Cont'd)



Click Next



Installing the Certificate (Cont'd)



Click Next



Installing the Certificate (Cont'd)



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

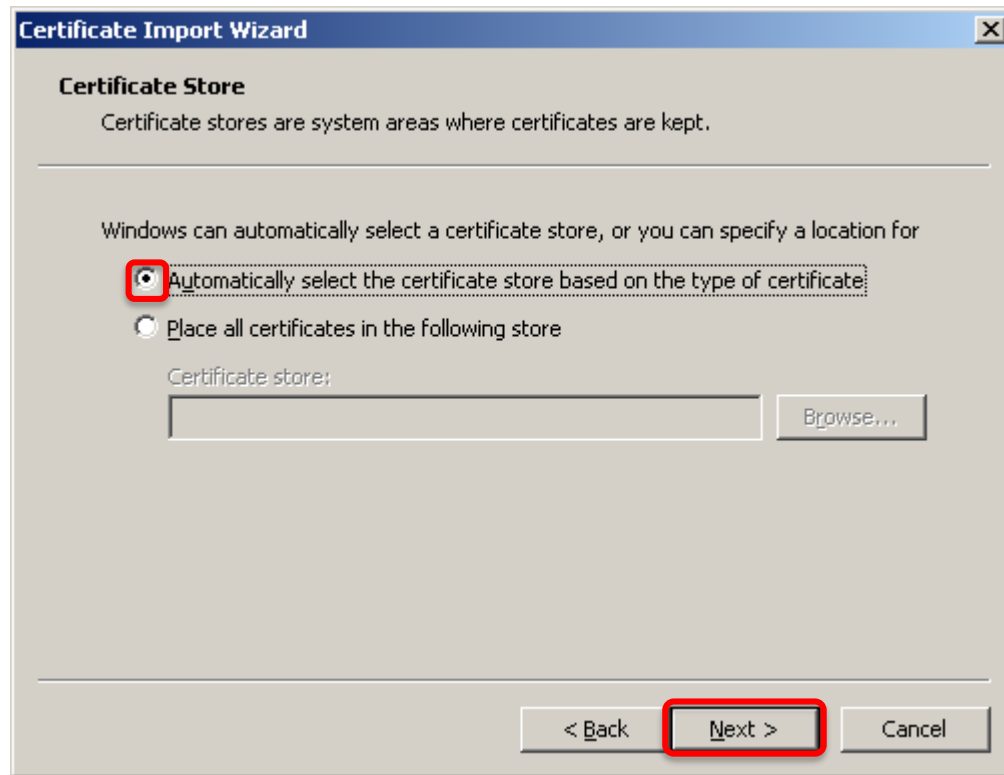
< Back **Next >** Cancel

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

If the first box is checked, you'll need to make a registry change which is **discouraged**



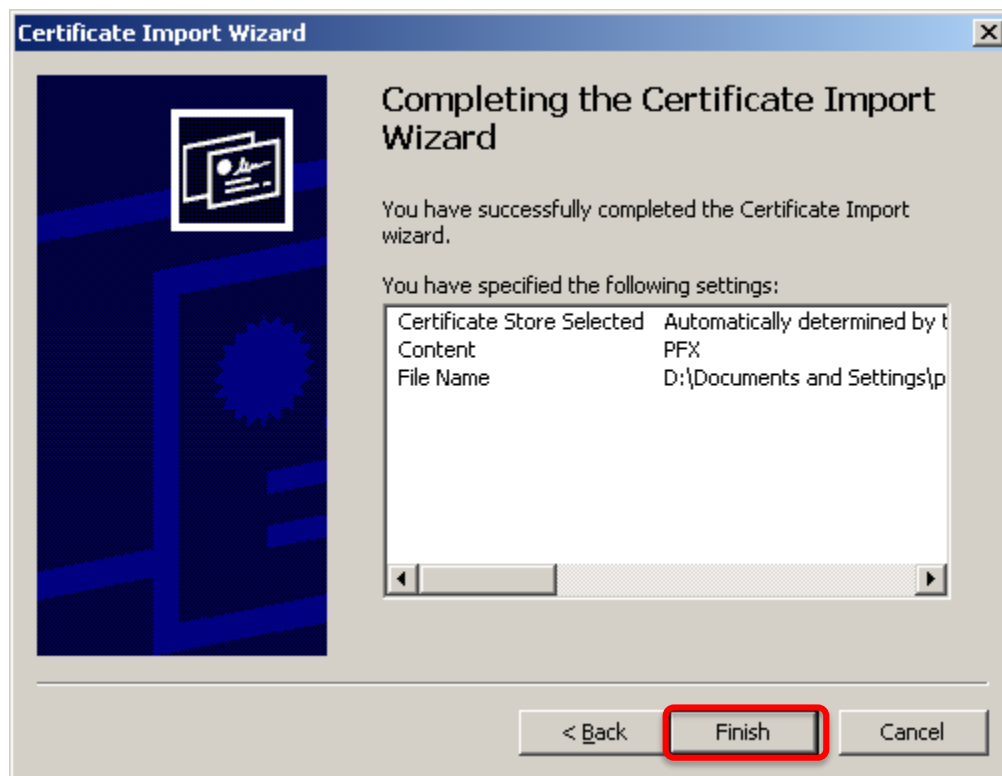
Installing the Certificate (Cont'd)



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*



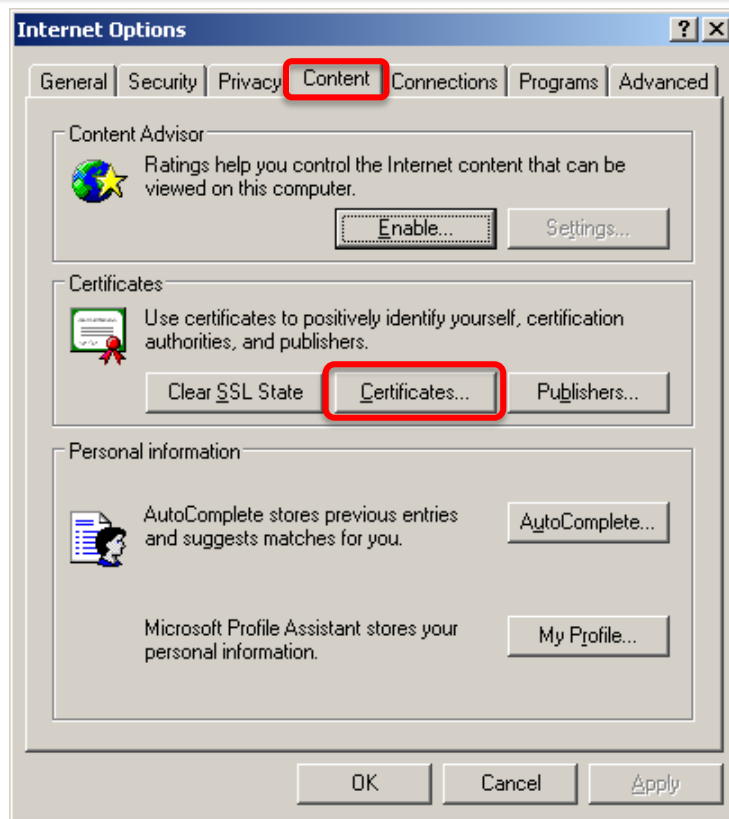
Installing the Certificate (Cont'd)



Click ***OK***



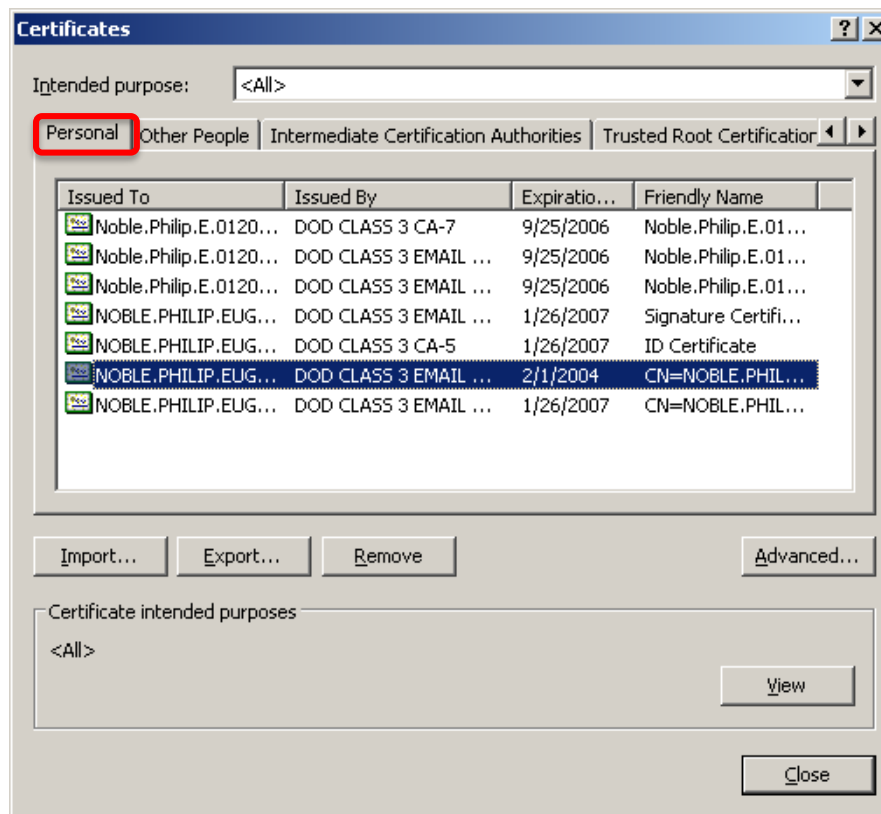
Verifying the Download



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



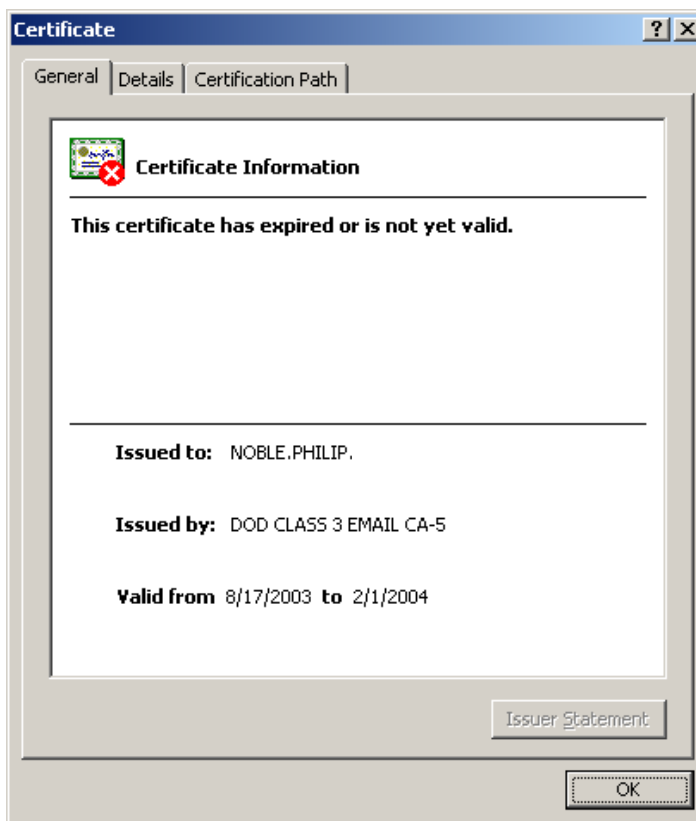
Verifying the Download (Cont'd)



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 a real bind as you may need to access old emails that were encrypted with / to your former CAC(s).

An idea for you is to follow slides 4-12, saving the file(s) to the computer you are on, and not run it. When you get to slide 11, 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 12-17 use 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.